COPY NO. 12

TECHNICAL REPORT 4556

FAULT TREE ANALYSIS

WALDEMAR F. LARSEN

JANUARY 1974

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

PICATINNY ARSENAL
DOVER, NEW JERSEY

The findings in this report are not to be construed as an official Department of the Army Position.

DISPOSITION

Destroy this report when no longer needed. Do not return to the originator.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (*When Data Entered*)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPDRT NUMBER
Technical Report 4556

2. 3OVT ACCESSION NO.

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (*and Subtitle*)
FAULT TREE ANALYSIS

5. TYPE OF REPORT & PERIOD COVERED

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(*s*)
Waldemar F. Larsen

8. CONTRACT DR GRANT NUMBER(*s*)

9. PERFORMING ORGANIZATIDN NAME ANO AODRESS
U. S. Army Picatinny Arsenal, Dover, New Jersey

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING DFFICE NAME AND AODRESS

12. REPORT OATE
January 1974

13. NUMBER OF PAGES
76

14. MONITDRING AGENCY NAME & AODRESS(*if different from Controlling Office*)

15. SECURITY CLASS. (*of this report*)
UNCLASSIFIED

15a. OECLASSIFICATION/DOWNGRAOING SCHEOULE

16. OISTRIBUTION STATEMENT (*of this Report*)
Approved for Public Release; Distribution Unlimited

17. DISTRIBUTION STATEMENT (*of the abstract entered in Block 20, if different from Report*)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (*Continue on reverse side if necessary and identify by block number*)

Fault tree analysis
Boolean algebra
Probability
Reliability
Logic diagram
Block diagram
Failure mode
Failure mechanism
XM813 Safety & Arming device
Sensitivity rating

20. ABSTRACT (*Continue on reverse side if necessary and identify by block number*)

This report describes the procedure to be used for constructing fault trees, the application of Boolean Algebra and the use of probability values in the final algebraic expressions.

While not the only method which can be used, the fault tree technique is considered to be a very effective analytical tool in assessing system safety.

This report supersedes Picatinny Arsenal Technical Report 3822.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (*When Data Entered*)

FOREWORD

Fault tree analysis provides a logical method for graphically presenting the chain of events leading to a system failure. One result of its application to a system is a mathematical model suitable for determining system safety and reliability from the event probabilities.

This handbook is an adaption of Picatinny Arsenal Technical Report 3822, "Fault Tree Analysis" prepared by Waldemar F. Larsen, and published November 1968. Consequently, many of the examples are for fuzes and safety and arming devices. The techniques discussed, however, are applicable to any system.

Since the Technical Report was published and used, some refinements of the technique have been made. These refinements comprise:

a. A clearer distinction between a failure mode and a failure mechanism as applied to fault trees.

b. A clearer definition of some fault tree symbols.

A new feature of this handbook is a different approach to the quantification of a fault tree anlaysis. This approach uses mathematical apportionment of probabilities of occurrence of components given a required end item probability of occurrence.

CONTENTS

Tables

Figures

OBJECTIVES

To present a method for analyzing safety and reliability problems through the use of fault trees.

To present the use of Boolean Algebra to solve the probability combinations of the fault tree.

To present numerical methods to quantify the fault tree analysis.

To present illustrations of fault tree analyses.

ABSTRACT

This report describes the procedure to be used for constructing fault trees, the application of Boolean Algebra and the use of probability values in the final algebraic expressions.

While not the only method which can be used, the fault tree technique is considered to be a very effective analytical tool in assessing system safety.

This report supersedes Picatinny Arsenal Technical Report 3822.

INTRODUCTION

The Greek philosopher, Aristotle, about 330 B. C. made a proposition that a logical statement is either true or false, but never partially true or false.

Over 100 years ago, in his book entitled "An Investigation of the Laws of Thoughts," published in London in 1854, George Boole developed a mathematical system involving logic. This system is now called Boolean Algebra. Unlike ordinary algebra variables which can assume an infinite number of values, Boolean Algebra variables can assume only one of two different values.

In the middle 1950's Bell Telephone Laboratories started developing the fault tree concept by constructing a logic diagram using Aristotle's proposition and Boolean Algebra to express the number of different events which lead to an undesired end event. In 1962 Bell published a report on the Minuteman Launch Control System Safety using the fault tree analysis.

Since that time fault trees have been used to analyze both safety and reliability of systems whether simple or highly complex.

A fault tree is a logic diagram based on statements which are either true or false, on or off, open or closed, good or bad, present or absent, etc.

The fault tree serves to identify the events on an AND/OR basis that contributes to a given final event. The Boolean Algebra is used to express the number of different events (single or combined) which lead to the end event.

While not the only method of analysis, fault tree analysis has been recognized as a powerful analytical tool. For this reason it is hoped that this handbook will acquaint its readers with a working knowledge of fault tree analysis.

LIST SUCCESSFUL EVENTS AND REQUIREMENTS

Before starting a fault tree analysis it is absolutely essential that the system to be analyzed is thoroughly understood by the analyst. One of the best ways of assuring that the functioning of the system is understood is to list in chronological order the sequence of events leading to success. This list should be complete, omitting no part of the operation.

A listing of the performance or safety requirements should complement the sequence of successful events. Both of these lists will give a full understanding of the proper functioning and the necessary requirements for use in making a systematic failure analysis.

BLOCK DIAGRAMS

The sequence of successful events list is given in narrative form. From this list, a block diagram for successful events is made. Within each block is given the terse description of one event. The description will consist of a subject, a verb and sometimes an object.

The blocks will be joined together in series or parallel or a combination of the two according to the functioning of the system.

The method of constructing a block diagram is best understood by studying the diagrams of the examples given on pages 44 through 68.

SAFETY FAULT TREES

A safety fault tree identifies the various sequence of events that will result in an item malfunction which endangers friendly personnel and/or material.

Before drawing a fault tree, select the malfunction (safety or reliability) to be investigated. An item may fail in several different ways, so it is essential that a fault tree clearly state the situation under investigation. For example, a fuze may detonate prematurely, usually the most serious case, or the munition may leak explosive, creating a fire hazard. Regarding reliability, the munition may be a dud, miss the target, or function at the wrong time.

Each of the different ways ~~an item~~ may fail in different configurations, or different phases of the life cycle may require a separate fault tree.

While these fault trees may be similar, they will vary in the significant contributing events, and it is these variations which make the fault tree analysis such a powerful tool.

To emphasize this very important point, consider (a) a fuze prematures prior to assembly to the warhead (b) a fuze prematures the warhead in the launcher versus (c) a fuze prematures the warhead at unsafe short distance downrange.

For situation (b) (premature in launcher) one branch of the fault tree states that the rotor must be prearmed, which aligns the explosive train, while the other branch states that the detonator must fire prematurely with the most likely cause being a short circuit to the detonator so that when the missile battery is activated, the "blow" is immediate.

For situation (c) (premature at unsafe short distance) in addition to the prearmed rotor as above, that branch of the fault tree would show that a "short time" arming of rotor would be another contributing event. The other branch shows that the detonator must fire prematurely with the most likely causes being a foreign conductor between the inner and outer ogive of the nose crush switch giving a delayed short circuit, or that the missile strikes an obstacle.

The important difference between situation (b) and situation (c) is the kind and the timing of the events.

The following examples of situations are given for guidance:

Safety

Fuze prematurely detonates rocket in launcher
Fuze prematurely detonates rocket before minimum safe distance downrange
Fuze prematurely arms during transportation, and/or rough handling
(See page 37 for life cycle situations).

Reliability

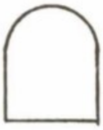
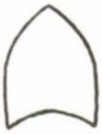
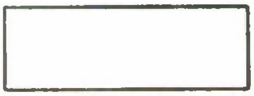
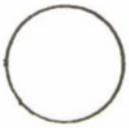
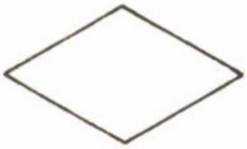
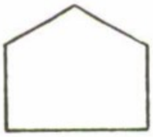
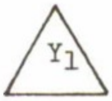
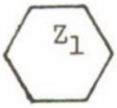
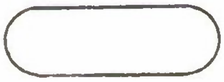
Fuze malfunctions at target impact
Fuze malfunctions at graze encounter
Fuze does not self-destruct missile

Fault Tree Construction

Conventional symbols have been established for constructing a fault tree. These symbols are listed in Table 1.

Table 1

Fault tree symbols

	A logical AND relation. (An AND gate.)	
	A logical OR relation. (An OR gate).	
	An event, usually undesirable, which is dependent upon a logically related set of sub-events. (A box)	
	An event which is usually a basic event or primary failure mode. (A circle)	Branches end with one of these symbols (or a repeat symbol)
	An event where analysis stopped. Further knowledge lacking or considered inconsequential. (A diamond)	
	An event that is normally expected to occur. (A house)	
	A repeat symbol indicating that the subset of functions influences more than one part of the tree within the same major branch. It is represented by the symbol Y with a numerical subscript. (A triangle)	
	A repeat symbol indicating that the subset of functions influences another part of the tree in a different major branch. It is represented by the symbol Z with a numerical subscript. (A hexagon)	
	A symbol applied to gates or events to record conditional or restrictive information concerning the symbol to which it is attached. (A flag)	

Gates are given numbers.

Events are given capital letters A through X.

The letters Y and Z are not used because they are used within the triangle and hexagon symbols. When there are more events than capital letters start over again using numerical subscripts (A_1 through X_1,A_2 through X_2).

Having determined the various possible end events and selected the order in which they will be considered, one is ready to start drawing the first fault tree.

To construct a fault tree it is suggested that a large piece of paper be obtained and that the first drawing of the fault tree be prepared freehand. Later it should be prepared in final form. Start at the top of the sheet and in the center draw a rectangle to represent the final event, usually a malfunction. Next draw a line down from the A box to an AND or an OR gate depending on the circumstances. From the gate draw lines down to the contributing events. Proceed in this manner until the branches reach a basic event or a primary failure mode or until it is needless to carry the analysis further.

Remember that to construct the fault tree start at the *top* and work down through the various branches.

Failure Modes and Failure Mechanisms

Ideally, branches of a fault tree should end at a failure *mode* or a basic event. It is important to note the difference between a failure mode and a failure mechanism. A failure mode is a *type* of failure while a failure mechanism is the *cause* of the failure. For example, the breaking of a gear tooth is a failure mode. The failure mechanism for the gear tooth breaking may be fatigue of metal initiated by a stress raiser resulting from grinding marks, inclusions, improper heat treatment and so on, or the gear tooth could break from a high impact load of from something jamming the gear train. All of these reasons are failure mechanisms, but the failure mode is simply the breaking of the gear tooth.

Another example of a failure mode would be an electric detonator not shorted when in fact it should be shorted.

For this, the failure mechanisms would be (a) shorting bar damaged or broken (b) improper soldering or (c) shorting bar missing.

To reiterate, fault tree branches are taken down to failure modes, but not to failure mechanisms. Once the failure mode has been identified on the fault tree a separate analysis should be made of the failure mechanism so proper safeguards can be taken during manufacturing, assembling, inspection and testing to eliminate the failure cause.

Basic Events

As mentioned above,a branch of the fault tree can end at a basic event which is not a failure mode. A basic event can be either of a normal or an abnormal nature. A normal basic event is an event which will happen every time the item is activated, such as a setback force or a missile battery activated or missile vibrations. These normally expected events would be placed within a "house" symbol.

An abnormal basic event can happen unexpectedly such as shock loading, static electricity, thermal or radio frequency initiation, or the missile striking an obstacle, etc. These abnormal basic events can be placed within the "circle" or "diamond" symbols depending upon the knowledge of the event.

Use of Boolean Algebra

Logic or Boolean Algebra is a fitting companion to the recently developed fault tree analysis. There are certain conventional symbols used in Boolean Algebra which are:

1 = True
0 = False
a, b, c, = Conditions or events
a' = "a" Prime meaning NOT a   If $a = 1$ then $a' = 0$
b' = "b" Prime meaning NOT b   If $b = 1$ then $b' = 0$

The basic relationships of Boolean Algebra are given in Table 2.

To analyze a fault tree by the use of Boolean Algebra start at the *bottom* of one of the branches and work *up*. Combine the individual events at the bottom according to whether they are connected by an AND gate or an OR gate. The AND gate combines the events by the (·) symbol and the OR gate combines the events by the (+) symbol. This procedure will be demonstrated in the examples on page 44 through 68.

Simplification of the Analysis

There are several techniques that can be used which will make the construction and the analysis of a fault tree simpler.

a. If the same contributing event occurs in two or more branches use the same identifying letter.

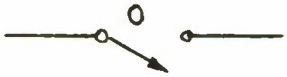
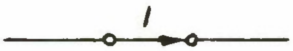
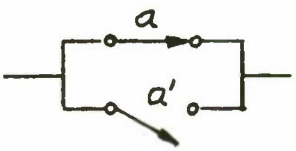
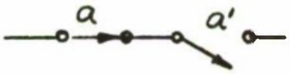
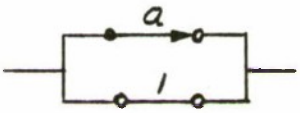
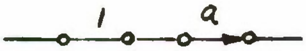
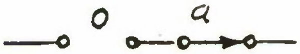
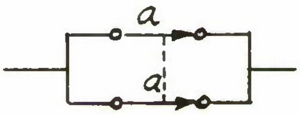
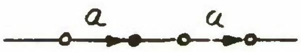
Table 2

Fundamental equations of Boolean Algebra

$+$ = OR

$\cdot$ = AND

(Elementary Propositions)

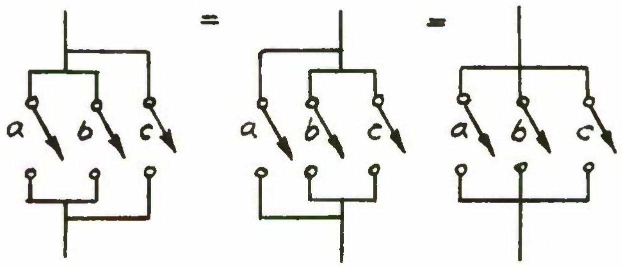
Code	Equation	Switch Analogy
I	$a' = 0$	
II	$a = 1$	
III	$a + a' = 1$	
IV	$a.a' = 0$	
V	$a + 1 = 1$	
VI	$a.1 = a$	
VII	$a.0 = 0$	
VIII	$a + a = a$	
IX	$a.a = a$	

(Associative Law)

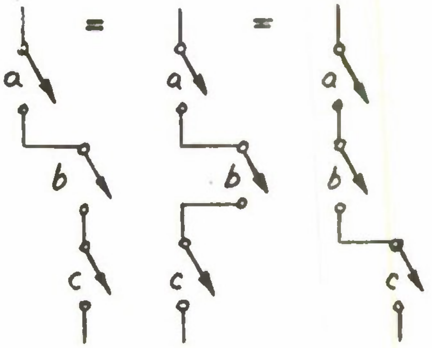
X $(a+b)+c =$

$= a+(b+c)$

$= a+b+c$

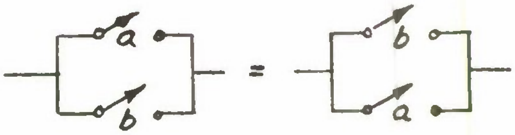


XI $a.(bc) = b.(ac) = c.(ab)$

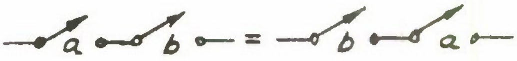


(Commutative Law)

XII $a + b = b + a$

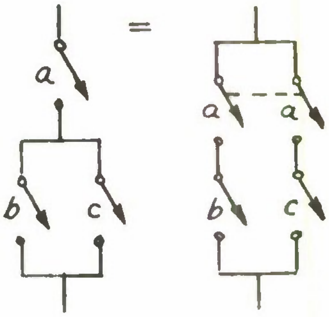


XIII $a.b = b.a$

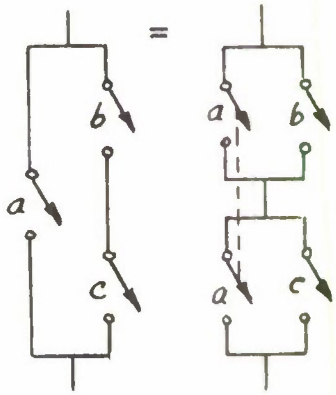


(Distributive Law)

XIV $a.(b+c) = ab + ac$

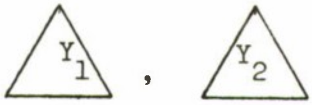


XV $a + bc = (a+b).(a+c)$

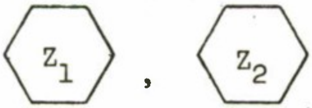


Interpretation of Equations. Code XIV example. The (+ = OR) symbol indicates a parallel circuit, while the (. = AND) symbol indicates a series circuit. The left hand circuit a.(b+c) shows that switch a AND either switch b OR c when closed would permit flow. The right hand circuit where a is a double pole, single throw switch would permit flow when switches a AND b, OR a AND c are closed.

b. Where a sequence of events occur in various branches of the fault tree after having been shown once for one branch they can be identified in other branches by the symbols



or



etc, depending on the circumstances. By the use of these repeat symbols both the construction and the analysis are simplified.

Examples of Simple Fault Trees

The introduction to the construction and analysis of fault trees is shown in two simple examples, Figures 1 and 2.

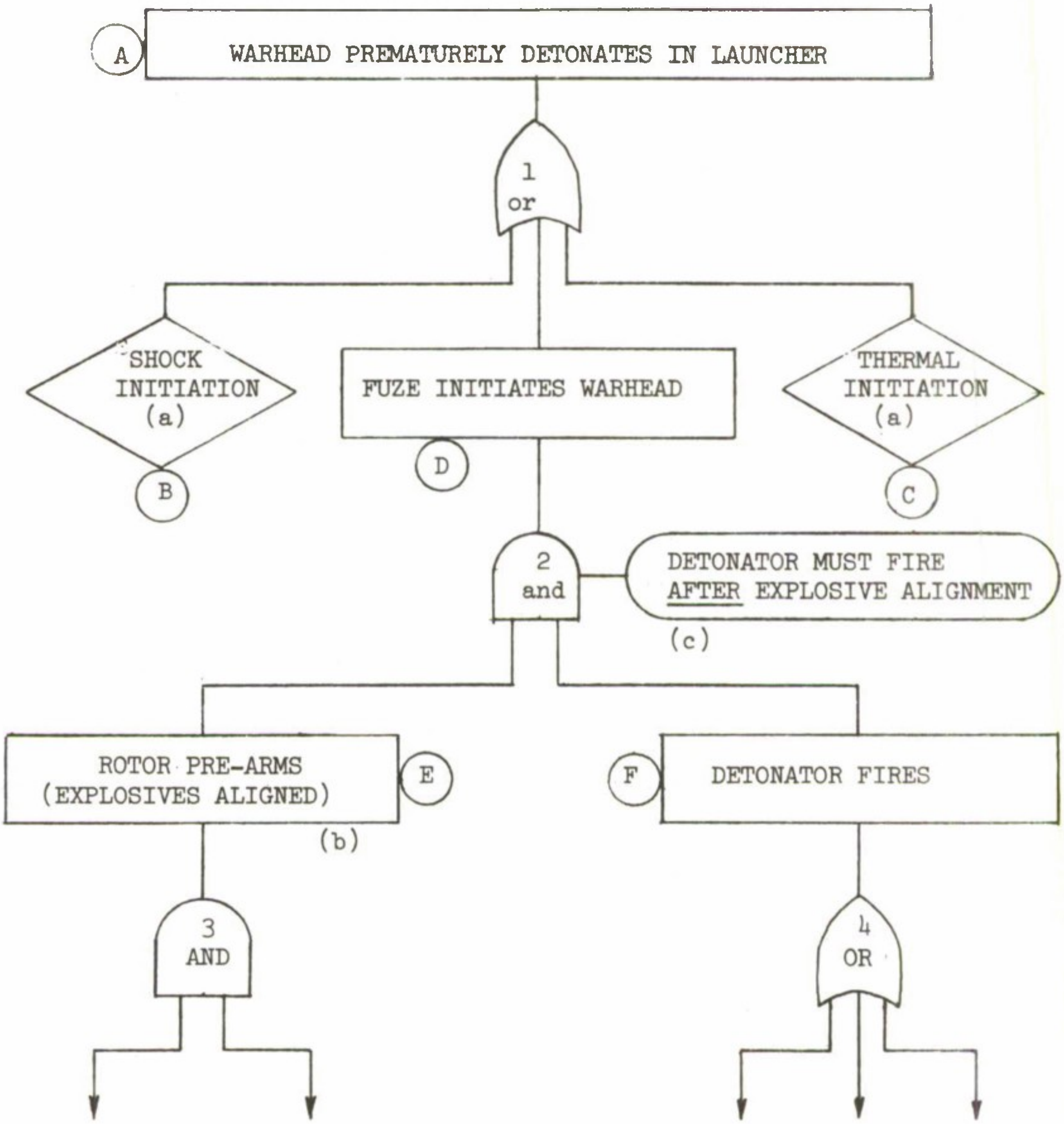
Figure 1 shows a warhead safety fault tree. Event A is the premature detonation of a warhead. OR gate #1 indicates that event A could be caused by events B, C, or D.

Event B, "Shock Initiation" and event C, "Thermal Initiation" were placed within the diamond symbols because further knowledge was lacking. Event D, "Fuze Initiates Warhead" was placed in a rectangle because it is known that this event can be caused by other contributing events. Event D is followed by the #2 AND gate because event E AND event F must happen simultaneously or event F must happen after event E to make event D occur. Events E and F are followed by the proper gates according to the knowledge of the system.

Still referring to Figure 1 a Boolean Algebra analysis is performed. Start at Gate (2)

$$(2) = E \cdot F \text{ (meaning E AND F)}$$
$$D = (2) = E \cdot F$$
$$(1) = B + C + D \quad \text{(meaning B or C or D)}$$
$$A = (1) = B + C + (2)$$
$$A = B + C + E \cdot F$$

Simply stated the resulting formula says that event A can be caused by event B, OR event C, OR events E AND F.



(a.) RELATIONSHIP BETWEEN THESE TWO EVENTS, IF ANY, WAS NOT EXPLORED.

(b.) "ALIGNMENT" APPLIES TO ANY POSITION WHICH PERMITS PROPOGATION FROM ONE EXPLOSIVE ELEMENT TO THE NEXT.

(c.) "AFTER" IMPLIES A TIME ELEMENT VARYING FROM A FRACTION OF A SECOND TO MANY HOURS.

Fig 1 Warhead safety fault tree

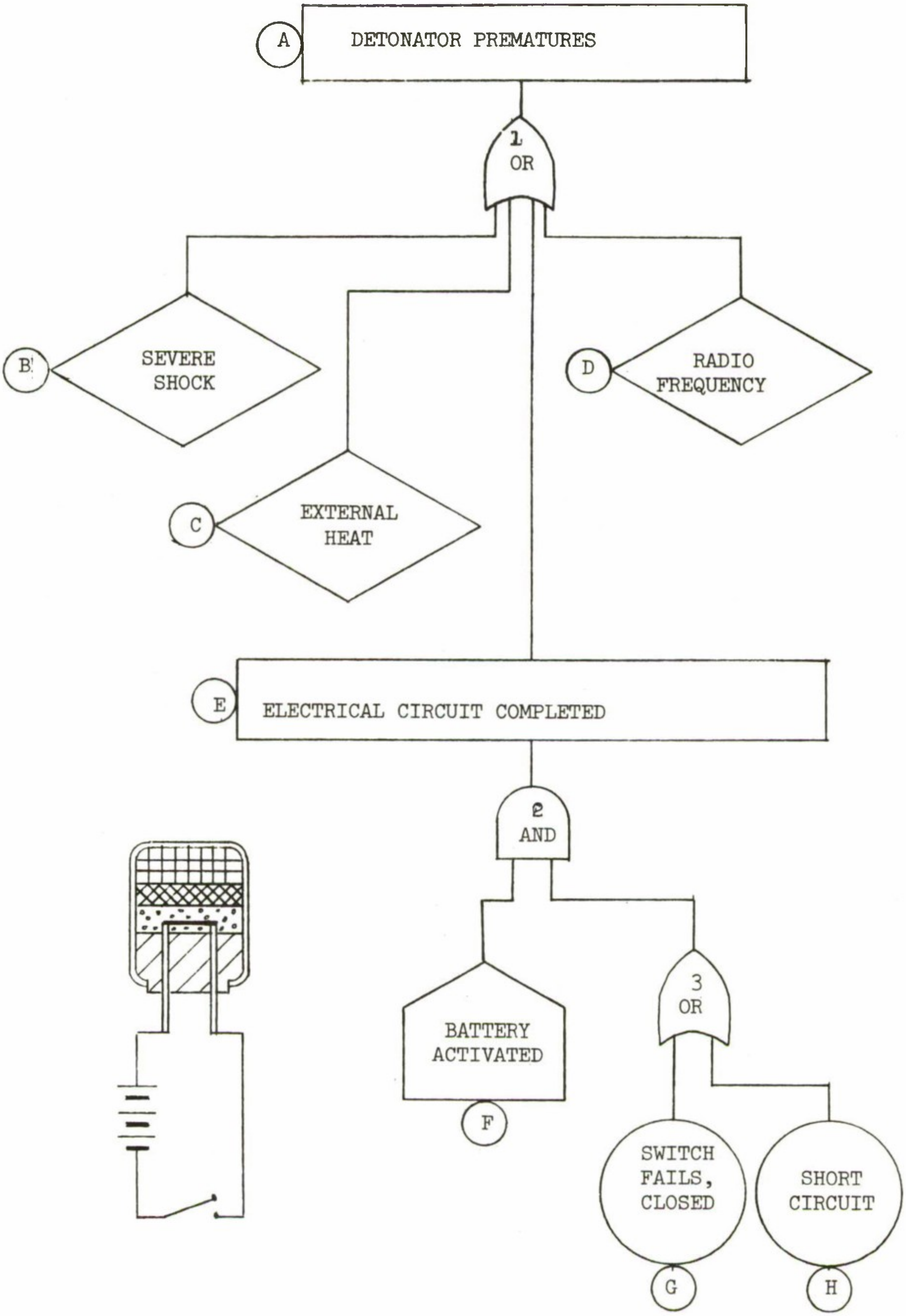


Fig 2 Detonator prematures fault tree

Next refer to Figure 2 which shows an electrical detonator premature fault tree. Two different symbols are used here; event F, "Battery Activated" which is a normal basic event placed in a "house" and event G, 'Switch Fails, Closed" and event H, "Short Circuit" which are primary modes of failure placed in "circles."

The analysis for this fault tree starts at Gate 3.

$$
\begin{aligned}
&(3) = G + H \\
&(2) = F \cdot (3) \\
&\qquad F \cdot (G + H) = FG + FH \\
&E = (2) \\
&A = (1) = B + C + D + E \\
&\qquad\quad = B + C + D + (2) \\
&\qquad\quad = B + C + D + F \cdot (G + H) \\
&\qquad\quad = B + C + D + FG + FH
\end{aligned}
$$

This formula says that event A can be caused by events B, *OR* C, *OR* D, *OR* F *AND* G, *OR* F *AND* H. In other words, an electrical detonator can premature because of severe shock, *OR* external heat, *OR* radio frequency, *OR* battery activated *AND* switch fails in the closed position, *OR* battery activated *AND* a short circuit.

The Probability of Final Event Occurrences

The Boolean Algebra equation, A = B + C + D + F (G + H) from Figure 2, expresses the single events or combination of events which could cause the final event "Detonator Prematures." Assuming that the probability value for each contributing event is known, it is not mathematically correct to directly substitute these directly into the above equation.

For two independent events, such as B and C, which are not mutually exclusive where either one or the other or both can occur, the final probability is expressed as:

$$P_A = P_B + P_C - P_{BC}$$

This means that the probability of A equals the probability of B plus the probability C minus the probability of B and C occurring at the same time.

It very often happens that the probability of occurrence is not known and other means must be used to determine a probability value. This value can always be subject to question.

The *product* of probabilities has very little effect on the primary *additive* terms. The fact that the selected values in many cases are not the actual values makes the added work of being mathematically correct unwarranted. Therefore, in making a safety analysis, the selected values will be substituted directly into the Boolean Algebra equation. Besides simplifying the work, the method used will give more pessimistic results than if the strictly correct mathematical method were followed.

Sensitivity Rating

After constructing a fault tree, one benefit which can be derived from it is to identify those input events which would have the most influence on the output fault. A visual inspection of the fault tree may not reveal the important input faults, but a simple calculation and the plotting of a graph can quickly show the relative sensitivity of the various inputs.

The steps to be taken in making the sensitivity rating calculation are:

1. Write the Boolean Algebra expression in the simplest form.

2. Substitute in the Boolean formula the probability value of 0.1 for each input event and solve to determine the probability value of the output fault.

3. Select a higher probability value (say 0.2, 0.5 or 1.0) and substitute this value for one input event, holding the other input events at 0.1 and solve for a new output fault probability value.

4. After doing step 3 for each input fault arrange the events in tabular form in descending order.

5. Divide the new output fault values by the output fault value with all inputs set at 0.1. This is called the Sensitivity Ratio.

6. The Sensitivity Rating is the quotient of the Sensitivity Ratio. This rating has no intrinsic value since the rating values change with the higher probability number chosen. However, the ratings do show the relative influence on the output fault.

7. Plot the probability of output fault values versus the probability of the input fault values. This will graphically display the sensitivity of the various input faults.

Two sample calculations follow, one for a fault tree with an OR gate feeding into the final event and the second for a fault tree with an AND gate.

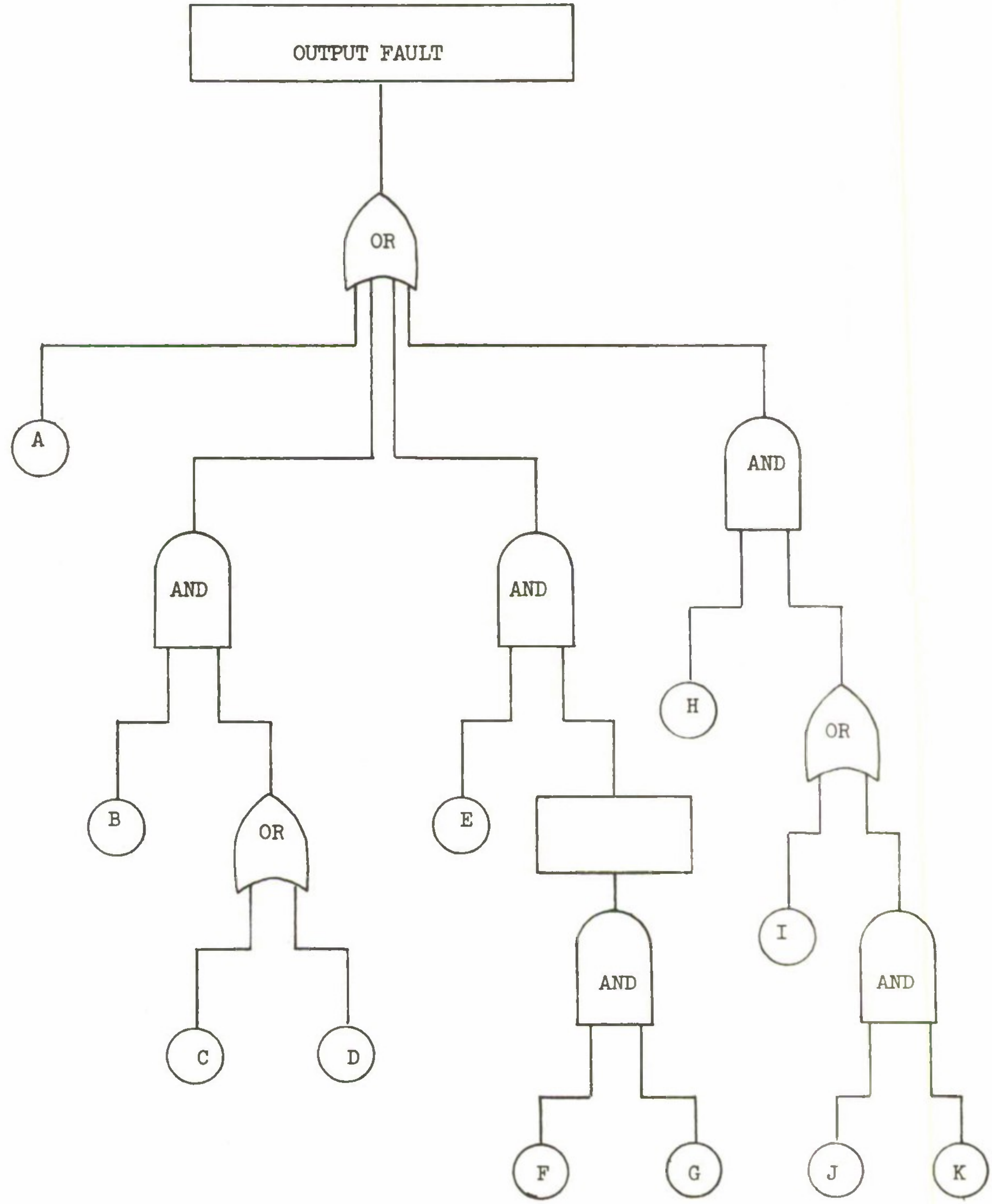


Fig 3 Sensitivity rating through OR gate fault tree

Thru *OR* Gate

$$P = A + B \cdot (C + D) + E \cdot F \cdot G + H(I + JK)$$

$$P = A + BC + BD + EFG + HI + HJK$$

Set all probabilities at .1

$$P = .1 + .01 + .01 + .001 + .01 + .001 = .132$$

Set each event at .5 – one at a time

Events changed		Probability of output fault
A = .5 + .01 + .01 + .001 + .01 + .001	=	.532
B = .1 + .05 + .05 + .001 + .01 + .001	=	.212
C or D = .1 + .05 + .01 + .001 + .01 + .001	=	.172
E,F, or G = .1 + .01 + .01 + .005 + .01 + .001	=	.136
H = .1 + .01 + .01 + .001 + .05 + .005	=	.176
I = .1 + .01 + .01 + .001 + .01 + .005	=	.172
J or K = .1 + .01 + .01 + .001 + .01 + .005	=	.136

Event	Sensitivity ratio	Sensitivity rating
A	.532 ÷ .132	4.03
B	.212 ”	1.61
H	.176 ”	1.33
C,D,I	.172 ”	1.30
E,F,G,J,K	.136 ”	1.03

Plot Graph

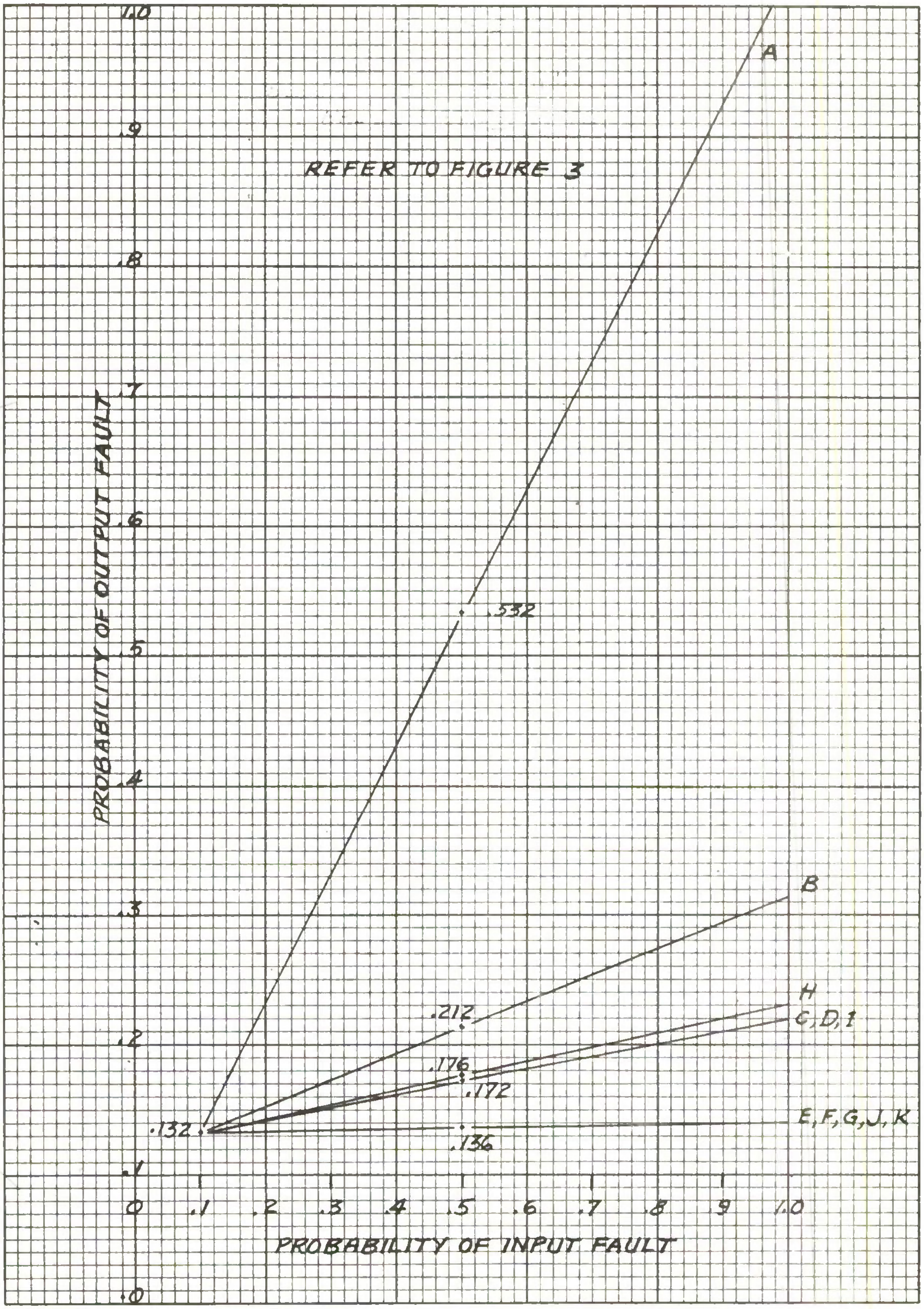


Fig 4 Sensitivity rating graph through an OR gate

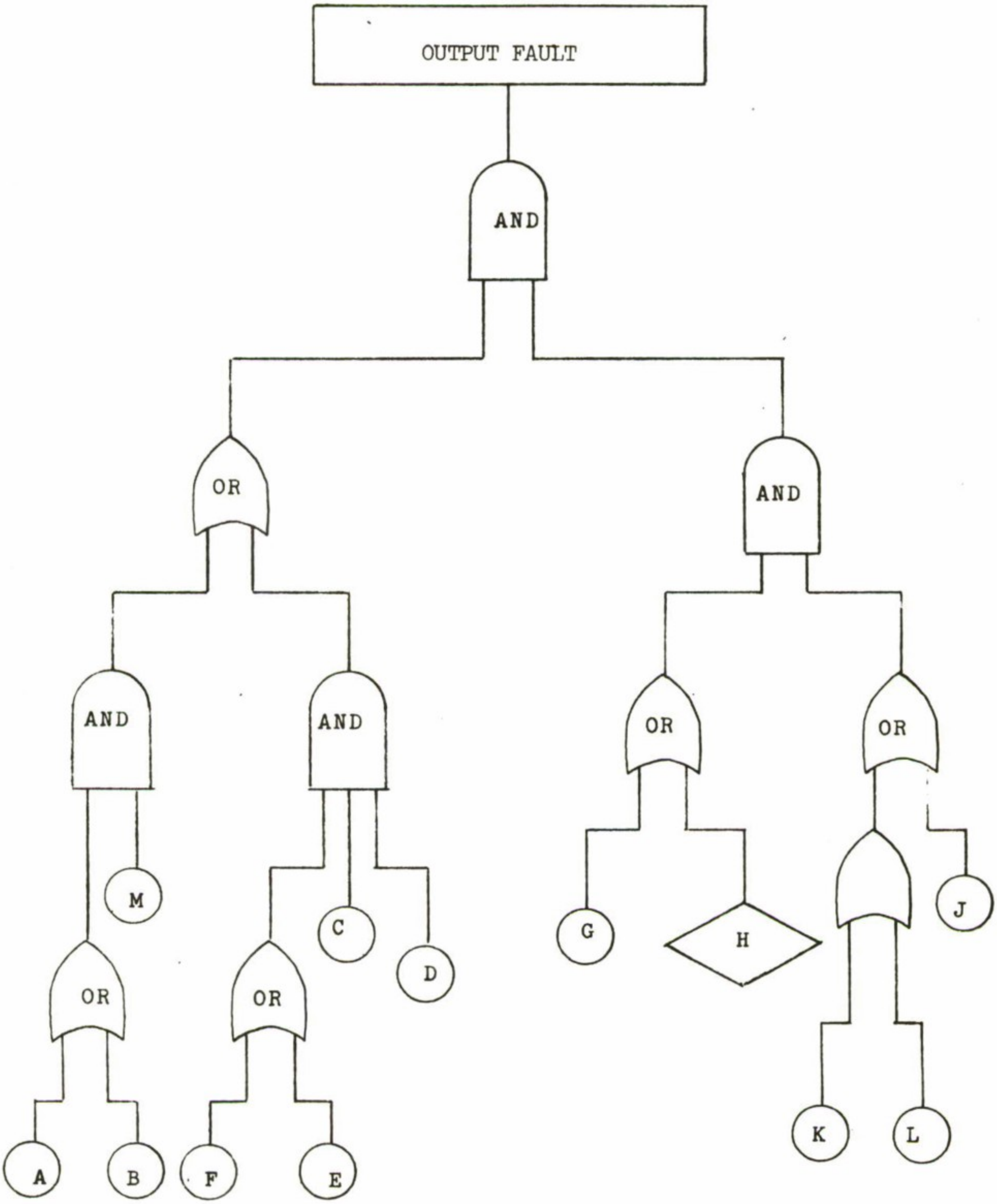


Fig 5 Sensitivity rating through AND gate fault tree

Thru *AND* gate

$$P = \left(\left[A+B\right] M + \left[E+F\right] CD\right) \cdot \left(\left[G+H\right]\left[J+K+L\right] \right)$$

$$P = (AM+BM+CDE+CDF) \cdot (GJ+GK+GL+HJ+HK+HL)$$

Set all probabilities at .1

$$P = (.01+.01+.001+.001) \cdot (.01+.01+.01+.01+.01+.01) = .00132$$

Set each event at 1.0 - one at a time

				Probability of output fault
M	=	(.1+.1+.001+.001) (.06)	=	.01212
G or H	=	(.022) (.1+.1+.1+.01+.01+.01)	=	.00726
A or B	=	(.1+.01+.001+.001) (.06)	=	.00672
J, K or L	=	(.022) (.1+.01+.01+.1+.01+.01)	=	.00528
C or D	=	(.01+.01+.01+.01) (.06)	=	.00240
E or F	=	(.01+.01+.01+.001) (.06)	=	.00186

Event	Sensitivity ratio	Sensitivity rating
M	.01212÷.00132	9.2
G,H	.00726 "	5.5
A,B	.00672 "	5.1
J,K,L	.00528 "	4.0
C,D	.00240 "	1.82
E,F	.00186 "	1.41

Plot Graph

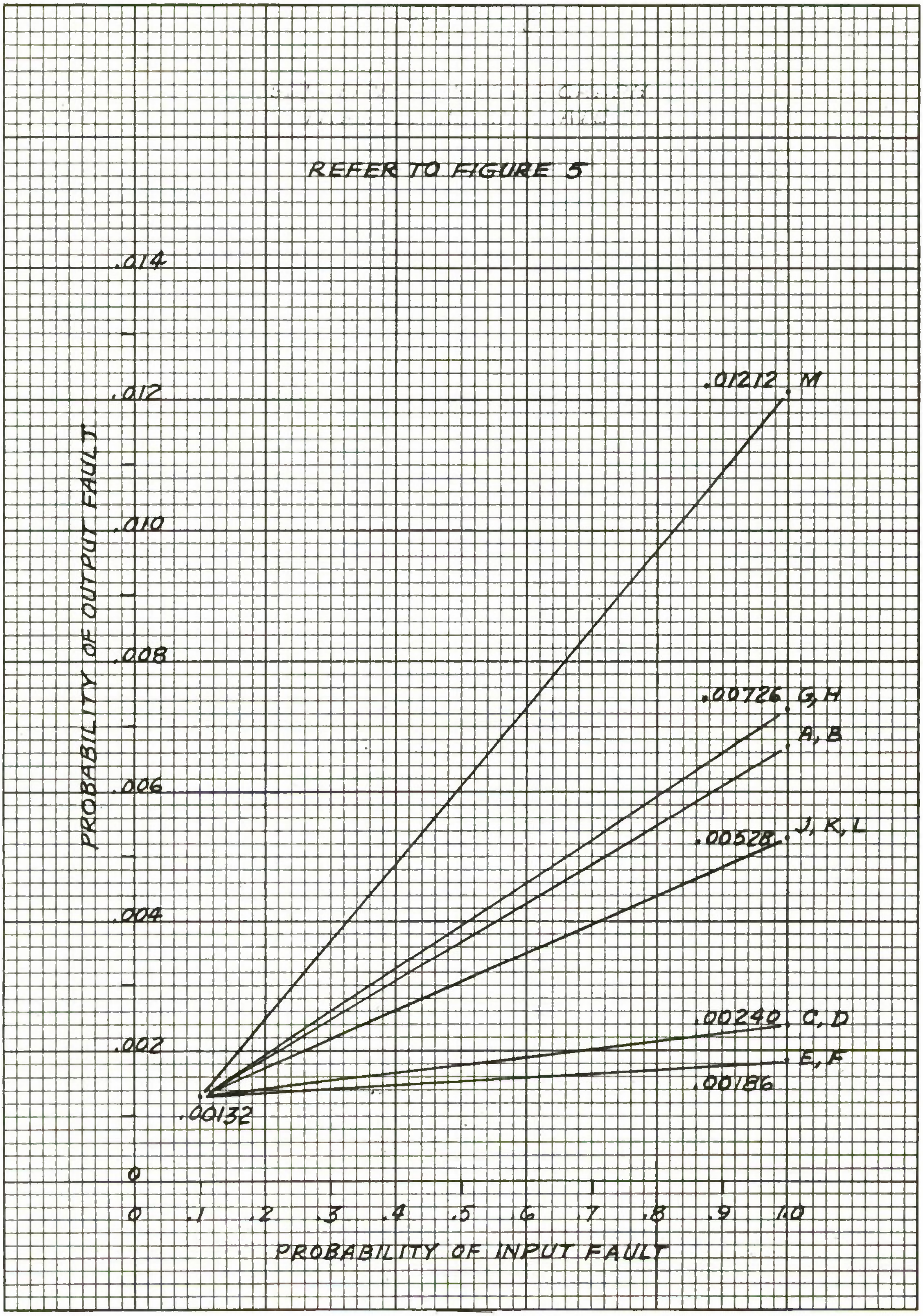


Fig 6 Sensitivity rating graph through an AND gate

Various Means for Selecting Event Probabilities

Engineering Judgment

In the absence of actual probability values for contributing failure modes or basic events, the next most natural thing to do is to select probabilities based on engineering judgment. This judgment may be based on knowledge or experience on a similar, but not exactly alike, item or situation. This has some validity. On the other hand, without prior knowledge the selection may have to be made by intuition or guess work. This is the poorest method.

To make sure that there is some semblance of uniformity in selecting the probability of occurrence, the following table is given as a guide:

Low probability = one malfunction in one or more million tests.

Example: $\frac{1}{1,200,000} = .000000833$

Average probability = one malfunction in one hundred thousand tests, more or less.

Example: $\frac{1}{105,000} = 00000952$

High probability = one or more malfunctions in ten thousand tests.

Example: $\frac{89}{10,000} = .0089$

Normal occurring event = 1.0

Example: Battery activated normally
Launch shock (setback)

By referring to Figure 2 we find six events which contribute to event A, the prematuring of an electric detonator. The Boolean algebraic expression already derived is:

$$A = B + C + D + F\,(G + H)$$

Engineering Judgment:

B = Severe shock (low) = .000001 = 1/1,000,000
C = External heat (average) = .00001 = 1/100,000
D = Radio frequency (low) = .000001 = 1/1,000,000
F = Battery activated (normal) = 1.0 = 1
G = Switch fails, closed (average) = .00002 = 1/50,000
H = Short circuit (high) = .0001 = 1/10,000

$$A = .000001 + .00001 + .000001 + 1.0\,(.00002 + .0001)$$
$$= .000132$$
$$= \frac{1}{7575}$$

This means that, on the basis of the hypothetical figures, the electrical detonator could premature once in 7575 times.

A careful study shows the influence that a normal occurring event and a high probability value event have on the final event.

Safety Apportionment, General

A catastrophic accident is never wanted but they can and do occur. It has become a practice to set a safety goal for each item which should be met or exceeded. For example, a safety goal may be not more than one accident in three million shots. The safety failure rate would then be expressed as $\frac{1}{3,000,000} = .0000003333$

Through Boolean algebra a mathematical model is derived for a particular fault tree which in turn yields equations for the various branches of the tree. If every event probability were known and put into the mathematical model the final event probability would be determined. Conversely, if the final event probability or safety goal has been established then the mathematical process can be reversed and the individual event probabilities determined. This reversing process is called apportionment. When the individual event probabilities are not equal, the problem of apportionment has an infinite number of solutions assuming no restrictions on the apportionment. Only when restrictions or relationships between the individual event probabilities have been established can a finite solution be made. From this point, trade-offs between individual event probabilities can be made. Because of certain constraints such as component costs, weights, or reliabilities, there will be some individual event allowable probabilities which cannot be readily varied. The mathematical techniques used to find the best combination vary in sophistication from trial and error to dynamic programing.

When event probabilities have been set through safety apportionment, it is being stated that an event must not happen more frequently than indicated. These are allowed probabilities for a given situation. A decision must be made whether or not a particular component can meet the assigned probability. If it is a critical component, that is, one that has a high influence on the output probability of the end event, it will be necessary to exercise special care in manufacture, assembly, inspection and testing of the item. Even after this, if the component still has a poor chance of meeting the assigned probability the design should be changed.

The various situations under which a safety apportionment can be made will be discussed in the following paragraph. Having made several apportionments the safety engineer must then decide on a final set of event probabilities.

The sample calculations which follow are for very simple situations. However, the principles involved can be used in more complex fault trees. To show how this is done see the XM813 analysis beginning on page 44 . Some variations illustrated there are:

a. Both branches and modes within branches equally likely.

b. All major events equally likely, some failure modes adjusted.

c. Branches unequal and failure modes adjusted.

Safety Apportionment – Fundamental Methods

Before investigating the various methods of making a Safety Apportionment, a review of some established fundamental methods would be in order. This can best be done by reviewing the mathematics used in determining system reliability.

The reliability of a *series* system is the product of the true reliabilities of the subsystems, i.e., $Rs = R_1 \times R_2 \times R_3 \ldots . \times R_n$

If each subsystem has the same reliability then:
$Rs = R_{il} \times R_{i2} \ldots . . \times R_{in} = R_i^n$

Conversely, apportionment is the determination of the subsystem reliabilities when the required system reliability (Rs) is given. If each individual subsystem has the same reliability then: $R_i = \sqrt[n]{Rs}$

Example: Given Rs = .98 for 3 equal subsystems in series.

$$R_i = \sqrt[3]{.98} = .9933$$

Check: $\boxed{.9933} \rightarrow \boxed{.9933} \rightarrow \boxed{.9933} \rightarrow .98$

When the subsystem reliabilities are not equal the problem of apportionment given an overall *series* system reliability has an infinite number of solutions assuming no restrictions on the apportionment. Only when restrictions or relationships between the individual subsystems have been established can a finite solution be made.

Failure Rates Unknown – Complexity or Relative Likelihood Apportionment Method – Series System

Very often the exact failure rate of a mechanical mechanism is not known. However, within a system the likelihood of a failure of an individual subsystem in relation to other subsystems may be known or assumed. Sometimes this relative likelihood is called complexity. The assumption of complexity may be based on several different factors. These factors could be:

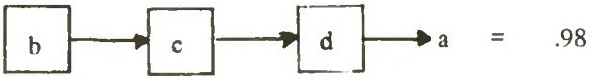
a. Number of components making up the subsystem

b. Difficulty of manufacturing the subsystem

c. Difficulty of inspecting the subsystem

d. Cost of the subsystem

A method has been developed which uses an index of the complexity numbers as "powers" of the system reliability (Rs). The sum of the indexes must equal one. This method is best illustrated by an example: It is desired to apportion reliabilities to three (3) subsystems so that the total system has a true reliability of .98 probability of success.



Assume that "c" is the most complex subsystem and is most likely to fail (least reliable), "b" is .73 times as likely to fail as "c" (more reliable), and "d" is .44 times as likely to fail as "c" (most reliable). Set up the following table.

Event	Relative complexity	Complexity index = i	Reliability apportionment = $(a)^i$
c	1.00÷ 2.17 =	.460	.99075*
b	.73	.336	.99324
d	.44	.204	.99589
	2.17	1.000	

$*c = (a)^i = .98^{.460}$

$.460 \log .98 = .460 \times \bar{1}.991226$

$= .460 \times 999.991226\text{-}1000$

$= 459.995964\text{-}460$

c = .99075
b = .99324
d = .99589

Check: a = b . c . d
= .99324 x .99075 x .99589 = .98000

The explanation of this method is based on the exponential law $a^m \cdot a^n = a^{m+n}$.

Thus:

$$Ra = Rb \cdot Rc \cdot Rd$$

$$Ra = Ra^{ib} \cdot Ra^{ic} \cdot Ra^{id}$$

$$Ra = Ra^{.336} \cdot Ra^{.460} \cdot Ra^{.204}$$

$$Ra = Ra^{(\,.336 + .460 + .204)\ = 1.0}$$

$$Ra = Ra^{1.0}$$

It is helpful to remember that a decimal number raised to a decimal power becomes a larger decimal number.

Failure Rates Known – Series System

If the true failure rates of the individual subsystem are known, then the true reliability of the whole system can be determined.

$$Rs = (1\text{-}F_1)(1\text{-}F_2)(1\text{-}F_3)\ldots\ldots(1\text{-}F_n)$$

If each subsystem has the same failure rate, then the above equation becomes:

$$Rs = (1\text{-}F(1\text{-}F)(1\text{-}F)\ldots\ldots\ldots\ldots(1\text{-}F_n)$$

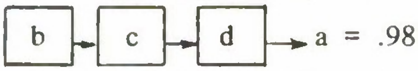
$$Rs = (1\text{-}F)^n$$

Example: The failure rate for 3 subsystems equals .0067 (.67%) each. Find system reliability

$$Rs = (1\text{-}.0067)^3 = .9933^3 = .980$$

If each subsystem has a different failure rate, then apportionment can be made for a given system reliability if a relationship is known between the failure rates of the subsystem.

Example: Given a system reliability = .98 for 3 subsystems in series.



"c" has the highest failure rate
"b" = .73 "c"
"d" = .44 "c"

$$Ra = (1\text{-}Fb)(1\text{-}Fc)(1\text{-}Fd) = .98$$

$$Ra = (1\text{-}.73Fc)(1\text{-}Fc)(1\text{-}.44Fc) = .98$$

Use Trial and Error Method

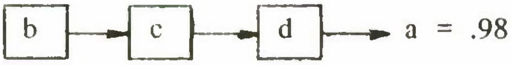
Let $Fc = .01$ $Ra = (1-.73x.01)(1-.01)(1-.44x.01)$
$(.9927)(.99)(.9956) = .978449$

Let $Fc = .0093$

$Ra = (1-.73x.0093)(1-.0093)(1-.44x0093)$
$(.993211)(.9907)(.995908) = .979948$ OK

Care must be exercised when using the Complexity or Relative Likelihood Apportionment Method that it is not used directly with reliability values but only with failure rates.

Example: Given a system reliability = .98 for 3 subsystems in series.



d has the highest reliability

b is 73% as reliable as d

c is 44% as reliable as d

$$\begin{aligned} Ra &= Rb \times Rc \times Rd = .98 \\ &= .73\, Rd \times .44\, Rd \times Rd = .98 \\ &= .321\, Rd^3 = .98 \end{aligned}$$

$$Rd^3 = \frac{.98}{.321} = 3.05$$

$$\begin{aligned} Rd &= \sqrt[3]{3.05} = 1.45 \\ Rb &= .73 \times 1.45 = 1.06 \\ Rc &= .44 \times 1.45 = .637 \end{aligned}$$

Check: $1.06 \times .637 \times 1.45 = .98$

Note that, according to this calculation, subsystem d has a reliability of 145% and b has a reliability of 106%. Obviously, this is wrong since no subsystem can have a reliability greater than 100%.

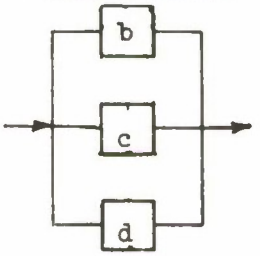
Safety Apportionment Through an AND Gate

The apportionment methods, just reviewed, dealt with system reliability with subsystems in series. Here system reliability was the *product* of the subsystem.

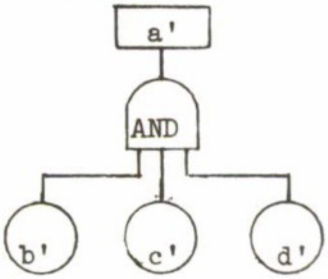
In dealing with fault trees the *product* of probabilities is found in a system where the subsystems are in a parallel circuit. De Morgan's law, as explained on page 41 describes this situation.

For purposes of illustration, assume a system with three (3) subsystems in parallel. The system and the corresponding fault tree would be:

BLOCK DIAGRAM



FAULT TREE



Reliability, $Ra = 1 - (Fb)(Fc)(Fd)$ where $F =$ failure rate

System Failure Rate, $a' = (b')(c')(d')$

Since fault trees are concerned with the probabilities of events and malfunctions of subsystems which contribute to an unwanted end event, the combination of these probabilities when going through an AND gate is the same as the probabilities of success in a series system. Therefore, the apportionment of probabilities through an AND gate is dependent on the *product* of the probabilities.

In general, two basic situations are encountered:

(1) All events are equally likely to happen, or in other words, all have equal complexity.

(2) All events have unequal complexity so that one subsystem is more likely to fail than another.

In the first situation of equal complexity, the safety apportionment of the subsystems in the n*th* root of the system safety goal where n is the number of subsystems.

Example: Safety requirements equal to or less than 1 premature in 3,000,000 shots in a parallel system consisting of 3 equal subsystems. See Figure 7.

Boolean Expression

$$a' = b' \,.\, c' \,.\, d' = \frac{1}{3,000,000} = .0000003333$$

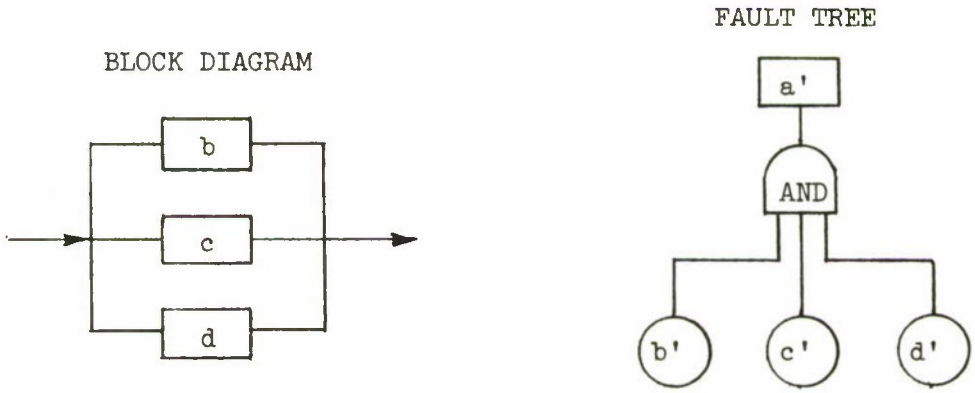
$$b' = c' = d' = (a')_{\frac{1}{n}} = \left(\frac{1}{3,000,000}\right)^{1/3} = \frac{1}{144.225}$$

This means that b' and c' and d' must have a failure rate or probability of occurrence equal to or less than 1 in 145 if the safety requirement of not more than 1 premature in 3,000,000 shots for the system is to be met.

In the second situation of unequal complexity the safety apportionment of the subsystems is obtained by proportioning the end item safety requirement as the power of the relative likelihood index of occurrence in the subsystems.

Example: Safety requirement equal to or less than 1 premature in 3,000,000 shots in a parallel system consisting of 3 subsystems where relative likelihood is $c' = 1.00$, $b' = .73$, $d' = .44$.

Calculations follow on next page


FAULT TREE

BLOCK DIAGRAM

Fig 7 Parallel system – apportionment through an *AND* gate

Safety Apportionment Through an AND Gate

Safety Requirement $\leq$ 1 premature in 3,000,000 shots

$$a' = b' \,.\, c' \,.\, d' = \frac{1}{3,000,000} = .0000003333$$

Event	Relative likelihood*		Likelihood index = i	Safety apportionment = $(a')^i$		
c'	$1.00 \div 2.17$	=	.460	.001048	=	$\frac{1}{954.2}$
b'	.73 "		.336	.006663	=	$\frac{1}{150.1}$
d'	.44 "		.204	.047715	=	$\frac{1}{20.96}$
	2.17		1.000	.000000333		$\frac{1}{3,000,000}$

$c' = (a')^i = .0000003333^{.460}$

$= .460 \text{ Log } .0000003333 = .460 \times \overline{7}.522835$

$= .460 \times (993.522835 - 1,000)$

$= 457.02050410 - 460$

$c' = .001048$

$b' = (a')^i = (a')^i = (.0000003333)^{.336} = .006663$

$d' = (a')^i = (.0000003333).^{204} = .047715$

Check:

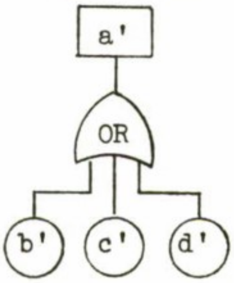
$a' = b' \,.\, c' \,.\, d' = .006663 \times .001048 \times .047715 = .0000003332$

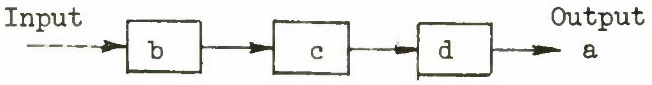
* Determined from prior knowledge

Safety Apportionment Through an OR Gate

Events and malfunctions of subsystems which pass through an OR gate for the end event to occur is derived from a *series* system. The system and the corresponding fault tree would be:

FAULT TREE





Reliability of this series system is:

$$Ra = Rb \times Rc \times Rd$$

Expressed in terms of failure rate this formula becomes:

$$Ra = (1-Fb)(1-Fc)(1-Fd)$$

Expanded, $Ra = (1-Fb-Fc-Fd+Fbc+Fcd+Fbd-Fbcd)$

The Boolean expression for this fault tree is:

$$a' = b' + c' + d'$$

A relationship exists between the Boolean expression and the expanded reliability formula if the second order and higher power values are dropped. The reliability formula then becomes:

$$Ra = (1-Fb-Fc-Fd)$$
$$Ra = 1-(Fb+Fc+Fd)$$

The parenthesis $(Fb+Fc+Fd)$ is the summation of the failure rates of the subsystems b, c,d and corresponds numerically to the Boolean expression $b' + c' + d'$. As discussed on page 13, this approximation is satisfactory when used with safety fault trees since it is on the pessimistic side. When used for reliability fault trees, this approximation will yield results which are less than the true reliability.

To make a safety apportionment for subsystems passing through an OR gate the following method can be used provided a relationship is known or assumed about the subsystems.

Again, two basic situations are encountered.

(1) All events are equally likely to happen, or in other words, all have equal complexity.

(2) All events have unequal complexity so than one subsystem is more likely to fail than another.

In the first situation of equal complexity, the safety apportionment of the subsystems is an equal division of the end-item safety requirement or goal.

Example: Safety requirement equal to or less than 1 premature in 3,000,000 shots. See Figure 8

$$a' = b' + c' + d' = \frac{1}{3{,}000{,}000} = .0000003333$$

$$b' = c' = d' = \frac{.0000003333}{3} = .0000001111 = \frac{1}{9{,}000{,}000}$$

This means that b'or c'or d'' must not have more than 1 premature in 9,000,000 shots if the safety requirement of not more than 1 premature in 3,000,000 shots for the system is to be met.

In the second situation of unequal complexity, the safety apportionment of the subsystems is obtained by multiplying the end item safety goal by the relative likelihood index of the subsystems.

Example: Safety requirement equal to or less than 1 premature in 3,000,000 shots in a series system consisting of 3 subsystems. Relative likelihood $c' = 1.000$, $b' = .73$, $d' = .44$.

$b' = .73\,c'$, $d' = .44\,c'$

Calculations follow on next page

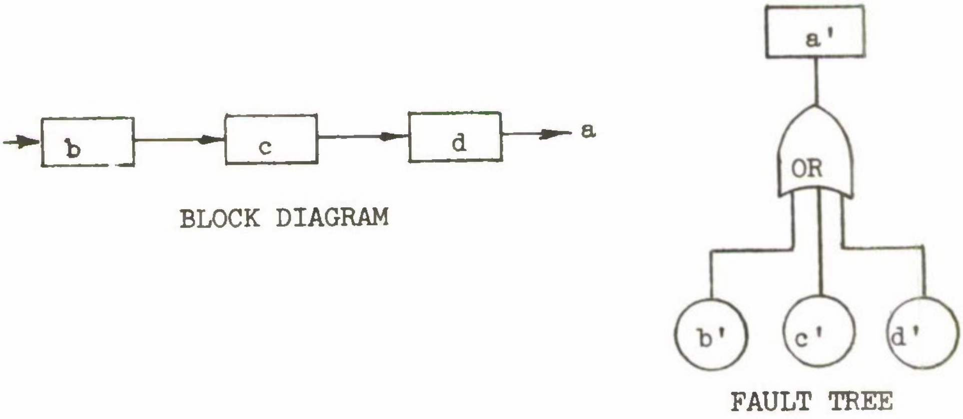
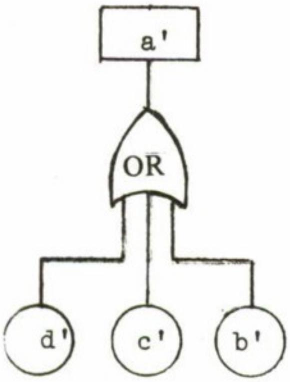


Fig 8 Series system apportionment through an OR gate

Apportionment Through an OR Gate



Safety Requirement $\leq$ 1 premature in 3,000,000 shots

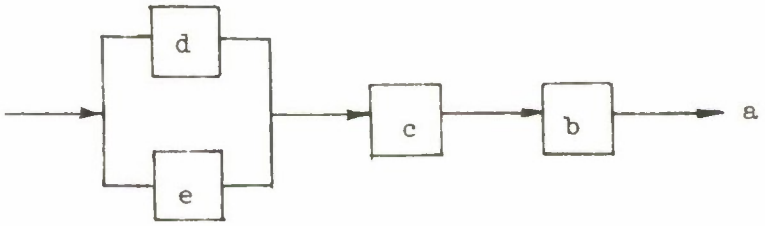
$$a' = b' + c' + d' = \frac{1}{3,000,000} = .0000003333$$

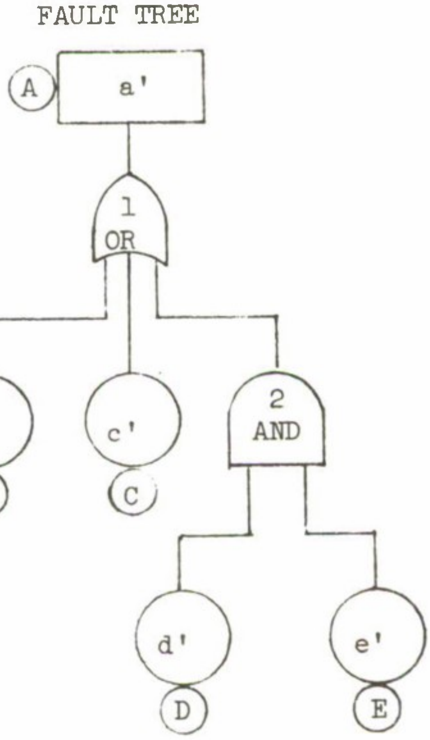
Event	Relative likelihood*	Likelihood index = i	Safety apportionment = ia'
c'	1.000 ÷ 2.17	.460	.0000001533 = $\frac{1}{6,523,157}$
b'	.73 "	.336	.000000112 = $\frac{1}{8,928,571}$
d'	.44 "	.204	.000000068 = $\frac{1}{14,705,882}$
	2.17	1.000	.0000003333 $\frac{1}{3,000,000}$

* Determined from prior knowledge

Safety Apportionment – All *OR* Gate Events Equally Likely

For a system which has a combination series - parallel circuit this method of safety apportionment assumes the situation that all events coming out of an *OR* gate are equally likely to occur. Any subsequent events out of an *AND* gate can be divided equally in probability, or they can be divided unequally if some relationship between them is known.





$a' = b' + c' + (2)$

$A = B + C + DE$

Fig 9 All OR gate events equally likely

All OR gate events equally likely (b$'$, c$'$, (2)

$$a' = b' + c' + (2) = \frac{1}{3{,}000{,}000}$$

If $b' = c' = (2)$

$$\text{Then } a' = b' + b' + b' = 3b' = \frac{1}{3{,}000{,}000}$$

$$b' = \frac{1}{3X3{,}000{,}000} = \frac{1}{9{,}000{,}000}$$

Check:

$$a' = \frac{1}{9{,}000{,}000} + \frac{1}{9{,}000{,}000} + \frac{1}{9{,}000{,}000}$$

$$= \frac{3}{9{,}000{,}000} = \frac{1}{3{,}000{,}000}$$

$$(2) = d' \cdot e' = \frac{1}{9{,}000{,}000}$$

If $d' = e'$ (equally likely)

$$\text{Then } D^2 = \frac{1}{9{,}000{,}000}$$

$$D = \left(\frac{1}{9{,}000{,}000}\right)^{1/2}$$

$$D = \frac{1}{3000} = .000333$$

Summary: Allowed Probabilities

A = .0000003333

B = .0000001111

C = .0000001111

D = .000333

E = .000333

If $e' = .45d'$ (unequal likelihood)

Then (2) $= d' . e' = d'(45d') = .45(d')^2$

$$D = \left(\frac{1}{.45X9,000,000}\right)^{1/2}$$

$$= \left(\frac{1}{4,050,000}\right)^{1/2} = \frac{1}{2012} = .0004970$$

$$E = .45 \text{ x } \frac{1}{2012} = \frac{1}{4471} = .00022366$$

Summary: Allowed Probabilities

A = .0000003333

B = .0000001111

C = .0000001111

D = .0004970

E = .00022366

Safety Apportionment - All Failure Modes Equally Likely

In a series – parallel circuit, refer to Figure 9, a situation can be assumed where all failure *modes* are equally likely to occur. The probabilities of B,C,D, and E are all equal.

$$a' = B + C + DE = \frac{1}{3,000,000}$$

By trial and error, each failure mode = .0000001666

Check:

$$a' = .0000001666 + .00000016666 + .0000001666^2$$
$$= .0000003332 + .0000000000000002775556$$
$$= .0000003332000277$$

Summary: Allowed Probabilities

A	=	.0000003333
B	=	.0000001666
C	=	.0000001666
D	=	.0000001666
E	=	.0000001666

Life Cycle Sets of Fault Trees

When conducting a safety failure analysis, to do a thorough job, it will be necessary to construct fault trees for every situation from the time the explosive elements are assembled into the item at the contractor's plant until the missile has had a safe separation from the launcher.

A typical example of a life cycle set of fault trees can be shown using a guided missile for an illustration.

Table 3

Complete set of safety fault trees

Number	Configuration		Rotor pre-arms	Detonator fires
1	S&A Device	Explosives loaded by mfgr.	a	j
2	S&A (loaded)	Shipped to warhead plant	b	k
3	S&A/Whd	S&A assembled to warhead	c	l
4	Fuze/Whd	Whd. Sect. shipped to missile plant	d	m
5	Fuze/Whd/Msl	Whd. Sect. assembled to missile	e	n
6	Fuze/Whd/Msl	Missile shipped to depot or field	f	o
7	Fuze/Whd/Msl	Missile fired in launcher	g	p
8	Fuze/Whd/Msl	Missile safely separated from launcher	h	q

S&A	=	Safety & Arming Device
Whd	=	Warhead
Msl	=	Missile

At first glance, it might seem a formidable job to construct eight fault trees, but actually it will not be that difficult because the hexagonal repeat symbols can be used from one tree to another. Just be sure that the Z's have the proper subscript for easy identification from tree to tree. It is important that a fault tree be constructed for each situation.

Gross Life Cycle Probabilities

Having constructed the complete set of safety fault trees listed in Table 3 the next logical question that can be asked is, "what is the probability of having a safety and arming device (or fuze) functioning prematurely from the time it is made until it safety separates from the launcher?" The answer to this question would give the gross life cycle probability of a hazardous premature.

Before deriving a solution to this problem look at the practical aspects of the operation of a fuze.

Most fuzes have a rotor or a slider whose explosive element must move into line with other explosive elements for proper propagation,and a detonator which must be initiated to start the propagation. If the rotor prematurely goes into line (arms) but the detonator does not fire,the fuze will not prematurely function. On the other hand, if the detonator fires prematurely when the rotor is not in line the fuze will not premature. In the latter case, only a dud will result and the fuze will no longer be hazardous.

Notice in Table 3 that two colums identify the condition of the rotor and the detonator in each of the eight situations. For example, the rotor could go into the armed position when the loaded item is being shipped to the warhead plant for assembly (identified as b). The fuze would premature if the detonator fired during shipment (k) or at any subsequent time, e.g., when the missile was triggered in the missile (p).

In statistical language, two events are called *mutually exclusive* if the occurrence of one excludes the occurrence of the other. The classic example is the drawing of an ace or king in a single draw. Since both ace and king cannot be drawn in a single draw the events are mutually exclusive. In this case, the rotor pre-arming and the detonator firing events are *not mutually exclusive* since the occurrence of one does not exclude the occurrence of the other. These two events are *independent events* because the occurrence or non-occurrence of one does not affect the probability of occurrence of the other. Also, there is a situation of *conditional probability* since a fuze premature can only happen if the detonator fires at the same time or after the rotor pre-arms, not *before* the rotor pre-arms.

The answer to the question posed at the start of this section for the gross life cycle probability of a fuze premature can be expressed in a practical and simplified formula as follows:

$$\begin{array}{rcccccccccccccc}
P_A = aj & + & ak & + & al & + & am & + & an & + & ao & + & ap & + & aq \\
 & + & bk & + & bl & + & bm & + & bn & + & bo & + & bp & + & bq \\
 & & & + & cl & + & cm & + & cn & + & co & + & cp & + & cq \\
 & & & & & + & dm & + & dn & + & do & + & dp & + & dq \\
 & & & & & & & + & en & + & eo & + & ep & + & eq \\
 & & & & & & & & & + & fo & + & fp & + & fq \\
 & & & & & & & & & & & + & gp & + & gq \\
 & & & & & & & & & & & & & + & hq
\end{array}$$

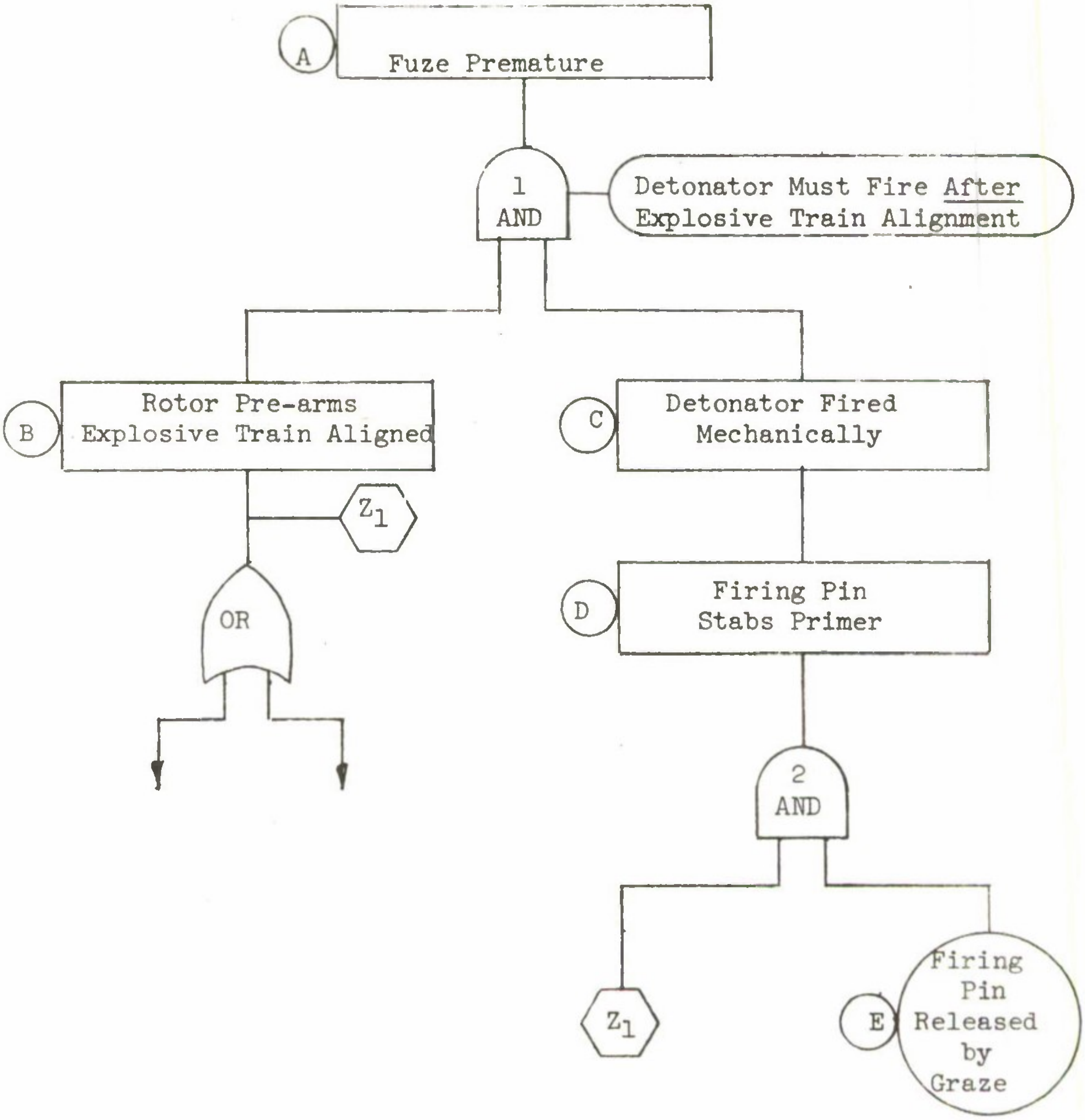
Caution in Using Repeat Events

When the probability values of the rotor pre-arming and the detonator firing events are considered separately to determine the gross life cycle probability *caution must be used in not combining repeat events.*

For example, suppose that a fuze has both an electrical detonator and a mechanical graze feature. The latter causes a firing pin to stab a primer when the projectile or missile strikes or glances off an obstacle. However, the firing pin cannot function unless the rotor has gone into the armed position. In the safe position, the rotor mechanically locks the firing pin and prevents it from moving. In many cases, the branches under the rotor pre-arms are identified by the repeat symbol.

This same repeat symbol could appear in the other branch of the fault tree under the event, "Detonator fired mechanically."

A simplified fault tree will show this:


A
Fuze Premature
1
AND
Detonator Must Fire After Explosive Train Alignment
B
Rotor Pre-arms Explosive Train Aligned
Z_1
OR
C
Detonator Fired Mechanically
D
Firing Pin Stabs Primer
2
AND
Z_1
E
Firing Pin Released by Graze

$$B = Z_1$$

$$C = D = (2) = Z_1 \cdot E$$

$$A = (1) = B.C$$
$$= Z_1 . (Z_1 . E) = Z_1 . Z_1 . E$$

But $Z_1 \,.\, Z_1 = Z_1$ by Code IX

Therefore, the probability *value* for Z_1 must not be used in the Detonator branch when calculating the probability value for a fuze premature. Event A then becomes $A = Z_1 . E$

RELIABILITY FAULT TREES

The discussion of fault trees so far has been directed at assessing the safety of a munitions item. It has been found advantageous to employ the same fault tree techniques in the analysis of reliability.

It has become a common practice in assessing reliability to make a block diagram of specific successful events leading to a specific reliable end event. Certainly, there is nothing wrong with this way of determining reliability. Generally, however, block diagrams do not show cnough detail of the unreliability of the various components which make up the complete assembly. The construction of a reliability fault tree investigates the unreliability of each important component. For this reason, the construction of a fault tree is a very valuable analytical tool for invcstigating reliability.

Relation Between Successful Events and Fault Trees

To show the relation betwcen the sequence of successful events and a fault tree analysis, consider a simple flashlight consisting of a bulb, a battery, and a switch. The sequence of successful events would be

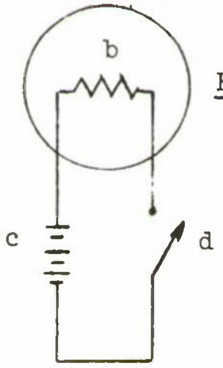
d = switch closed
c = battery activated
b = bulb filament heated
a = light beam produced

The flashlight is a serics circuit and if any of the components fail to function properly, event "a" will not occur, that is, the flashlight will not light.

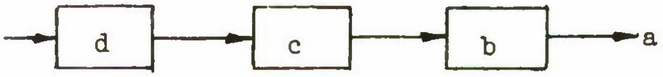
The fault tree analysis would bc:

a' = light beam not produced
b' = bulb filament broken or burned out
c' = battcry dead
d' = switch defective

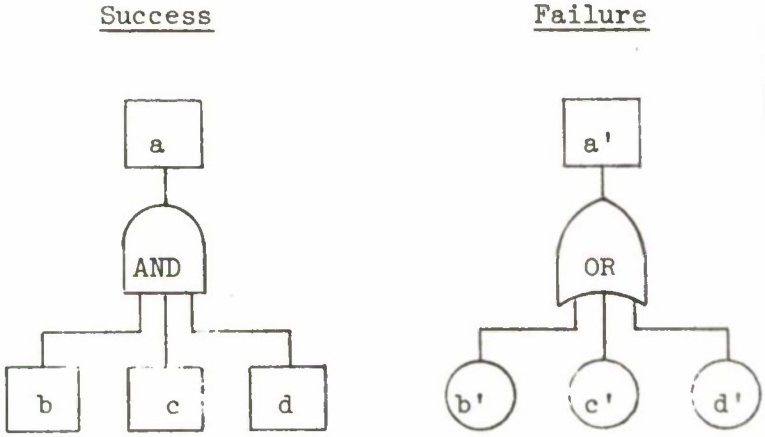
The above situations can be diagrammed thus:



Block Diagram (Successful Events)



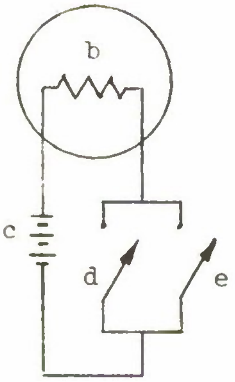
Tree Analysis


Success

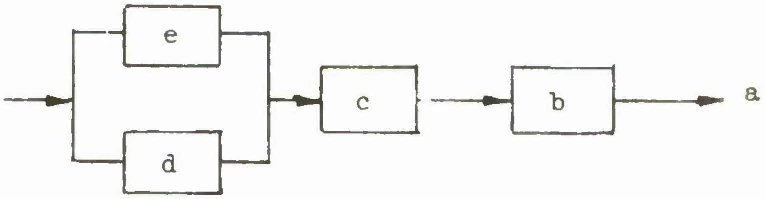
Failure

Boolean Algebra $a = b \cdot c \cdot d$ $a' = b' + c' + d'$

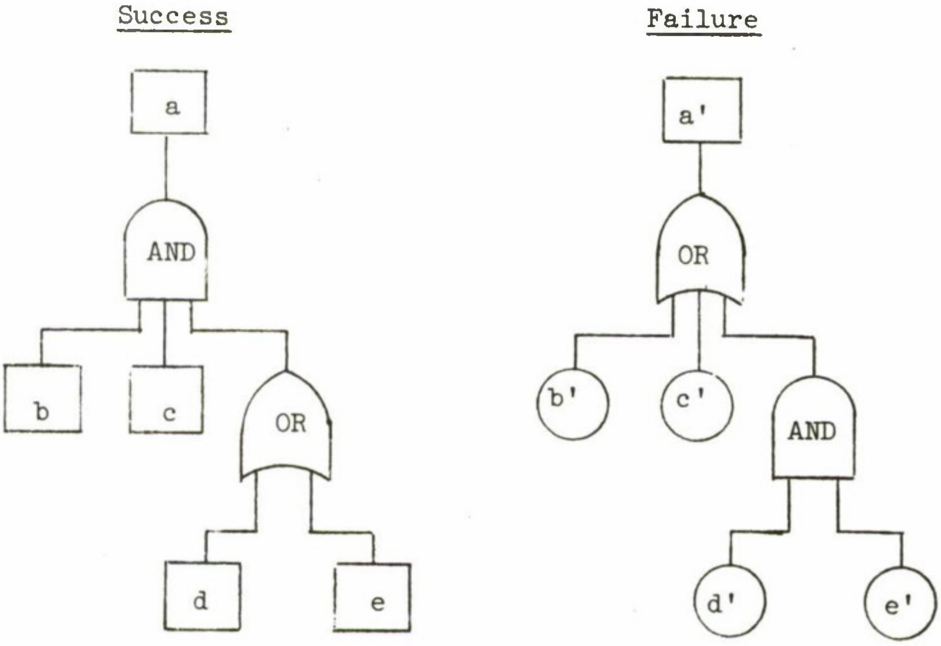
Assume that to improve the reliability of the switch a second switch was added in parallel with the first one, then the following comparison could be made:



Block Diagram (Successful Events)



Tree Analysis


Success

Failure

Boolean Algebra $a = b.c.(d+e)$ $a' = b' + c' + (d'.e')$

A study of these diagrams will show that *AND* gates for successes becomes *OR* gates for failures, and *OR* gates for successes become *AND* gates for failures. In Boolean Algebra this can be expressed as

$$(a.b.c....n)' = a' + b' + c'....+n'$$
$$(a + b + c....+n)' = a' .b' .c'.....n'$$

These two unique laws can be applied only to Boolean Algebra and are known as DeMorgan's laws.

FAULT TREE ANALYSIS FOR SAFETY AND ARMING DEVICE, XM813

The Safety and Arming (S&A) Device, XM813, was selected as an example because it is a relatively simple mechanism. To generalize the following systematic safety failure analysis procedures, the XM813 performance characteristics for arming times, arming distances and g levels will be indicated by letter symbols instead of numbers. The letter symbols to be used are:

t seconds = minimum arming time
T seconds = maximum arming time
d feet = minimum arming distance
D feet = maximum arming distance
N g's = maximum acceleration for non-arm condition
X g's = minimum constant acceleration to arm
Y g's = peak acceleration experienced

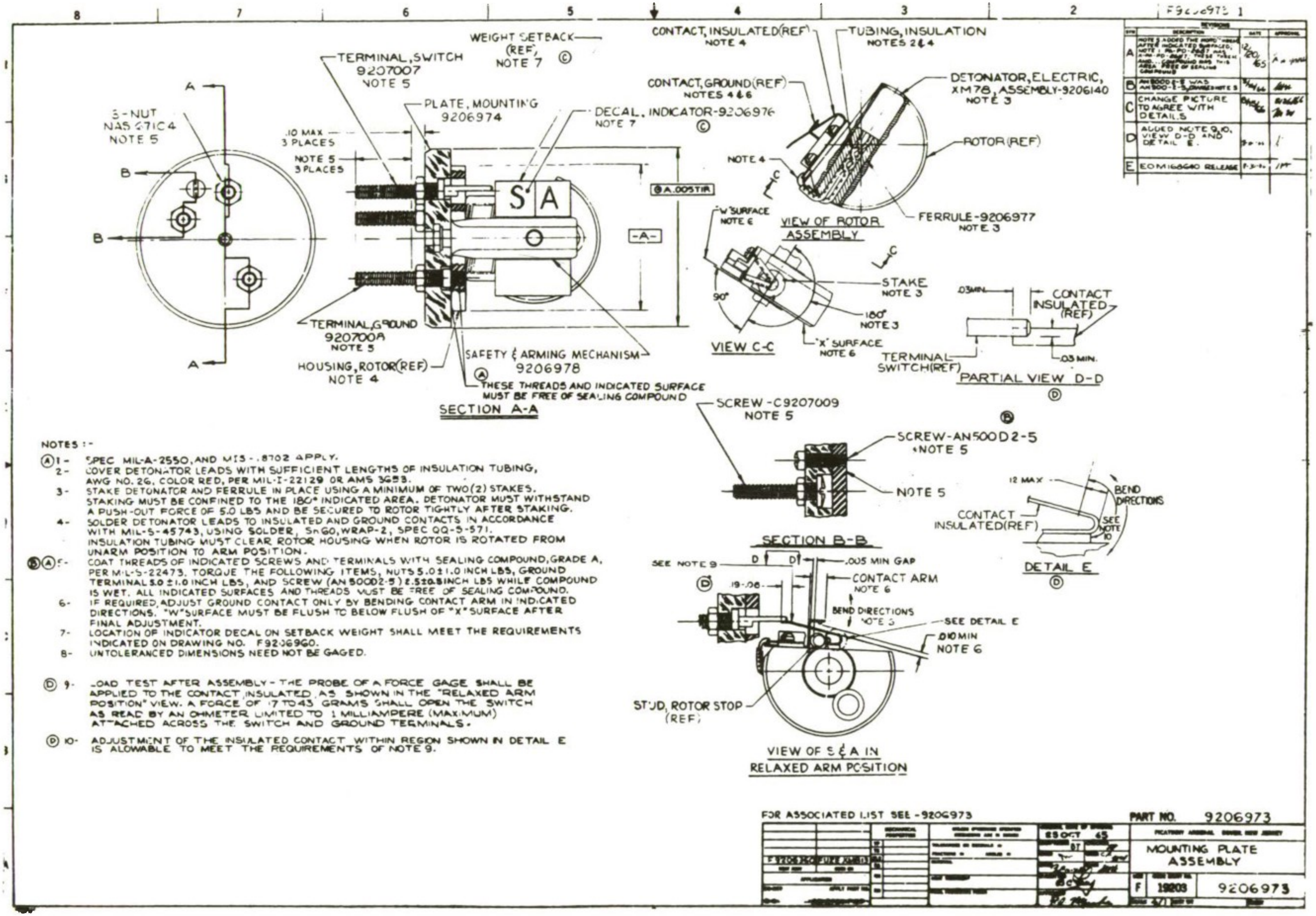
Description of XM813 S&A Device

The XM813 S&A device, Figure 10, is an hermetically sealed unit which contains a mechanical acceleration sensing mechanism. The explosive train consists of an electrically initiated detonator in an unbalanced rotor and a lead fixed in the base of the housing. The rotor has a cantilever switch which shorts the detonator in the unarmed position and completes the electrical circuit to the detonator when in the armed position. A clock mechanism controls the rotation of the rotor. One brass bias weight which unlocks the rotor at setback is restrained by two helical compression springs mounted on the bias weight guide posts. The bias weight has a decal with the letters "S" and "A" that can be viewed through a port in the housing to determine visually whether the unit is in the armed or un-armed position. Electrical power is supplied by an on-board missile battery. When the double ogive of the missile is crushed at impact, the electrical circuit is completed through the S&A wire harness. (See Fig 11.)

Sequence of Successful Events

The gunner triggers the launch operation. The thermal battery, which supplies electrical energy for the S&A device, is activated.

At launch, the missile is subjected for a short time to a high acceleration of Y g's. The resulting force causes the bias weight to overcome the spring force.



NOTES :-

Ⓐ1- SPEC MIL-A-2550, AND MIS-.8702 APPLY.

2- COVER DETONATOR LEADS WITH SUFFICIENT LENGTHS OF INSULATION TUBING, AWG NO. 26, COLOR RED, PER MIL-I-22129 OR AMS 3653.

3- STAKE DETONATOR AND FERRULE IN PLACE USING A MINIMUM OF TWO (2) STAKES. STAKING MUST BE CONFINED TO THE 180° INDICATED AREA. DETONATOR MUST WITHSTAND A PUSH-OUT FORCE OF 5.0 LBS AND BE SECURED TO ROTOR TIGHTLY AFTER STAKING.

4- SOLDER DETONATOR LEADS TO INSULATED AND GROUND CONTACTS IN ACCORDANCE WITH MIL-S-45743, USING SOLDER, Sn60, WRAP-2, SPEC QQ-S-571. INSULATION TUBING MUST CLEAR ROTOR HOUSING WHEN ROTOR IS ROTATED FROM UNARM POSITION TO ARM POSITION.

ⒷⒶ5- COAT THREADS OF INDICATED SCREWS AND TERMINALS WITH SEALING COMPOUND, GRADE A, PER MIL-S-22473. TORQUE THE FOLLOWING ITEMS, NUTS 5.0±1.0 INCH LBS, GROUND TERMINAL 5.0±1.0 INCH LBS, AND SCREW (AN500D2-5) 2.5±0.5 INCH LBS WHILE COMPOUND IS WET. ALL INDICATED SURFACES AND THREADS MUST BE FREE OF SEALING COMPOUND.

6- IF REQUIRED, ADJUST GROUND CONTACT ONLY BY BENDING CONTACT ARM IN INDICATED DIRECTIONS. "W" SURFACE MUST BE FLUSH TO BELOW FLUSH OF "X" SURFACE AFTER FINAL ADJUSTMENT.

7- LOCATION OF INDICATOR DECAL ON SETBACK WEIGHT SHALL MEET THE REQUIREMENTS INDICATED ON DRAWING NO. F9206960.

8- UNTOLERANCED DIMENSIONS NEED NOT BE GAGED.

Ⓓ 9- LOAD TEST AFTER ASSEMBLY - THE PROBE OF A FORCE GAGE SHALL BE APPLIED TO THE CONTACT, INSULATED, AS SHOWN IN THE "RELAXED ARM POSITION" VIEW. A FORCE OF 17 TO 43 GRAMS SHALL OPEN THE SWITCH AS READ BY AN OHMMETER LIMITED TO 1 MILLIAMPERE (MAXIMUM) ATTACHED ACROSS THE SWITCH AND GROUND TERMINALS.

Ⓓ 10- ADJUSTMENT OF THE INSULATED CONTACT WITHIN REGION SHOWN IN DETAIL E IS ALOWABLE TO MEET THE REQUIREMENTS OF NOTE 9.

REVISIONS

SYM	DESCRIPTION	DATE	APPROVAL
A	NOTE 5 ADDED THE WORD "WHILE" AFTER INDICATED SURFACES; NOTE 1 [illegible] WAS [illegible]. THESE THREADS AND ... COMPOUND WAS THIS AREA FREE OF SEALING COMPOUND	12/20/65	[illegible]
B	AN500D2-5 WAS AN500-2-5, CHANGE NOTE 5	[illegible]	[illegible]
C	CHANGE PICTURE TO AGREE WITH DETAILS	[illegible]	[illegible]
D	ADDED NOTE 9, 10, VIEW D-D AND DETAIL E.	[illegible]	
E	EOM168640 RELEASE	[illegible]	[illegible]

FOR ASSOCIATED LIST SEE -9206973

PART NO. 9206973

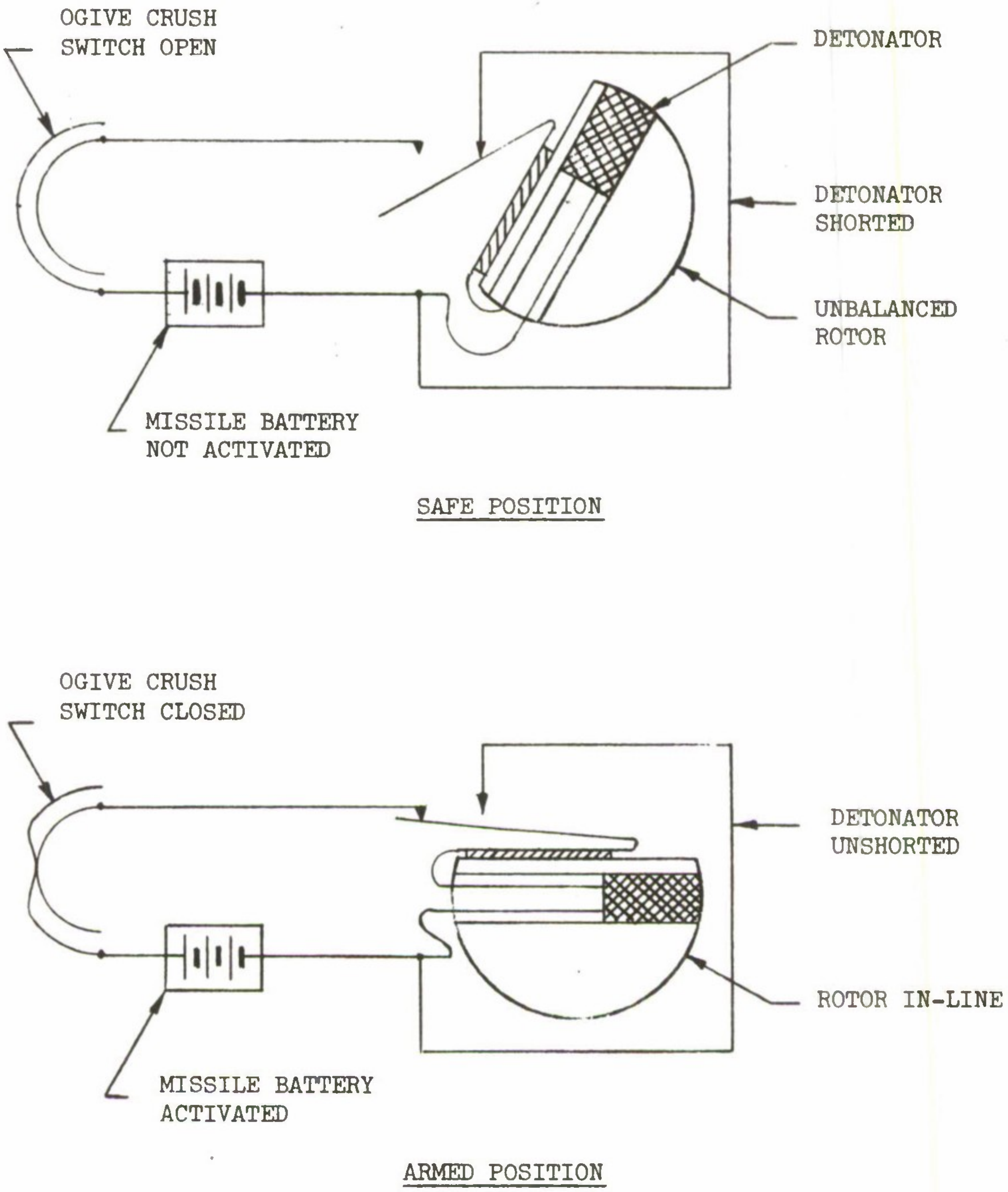
PICATINNY ARSENAL DOVER, NEW JERSEY

MOUNTING PLATE ASSEMBLY

F 19203 9206973

28 OCT 65

Fig 10 XM813 S&A device mounting plate assembly



SAFE POSITION

ARMED POSITION

Fig 11 XM813 Schematic

When setback moves the bias weight, the rotor is unlocked and the arming cycle starts. The annular gear on the unbalanced rotor engages the runaway escapement of the arming mechanism.

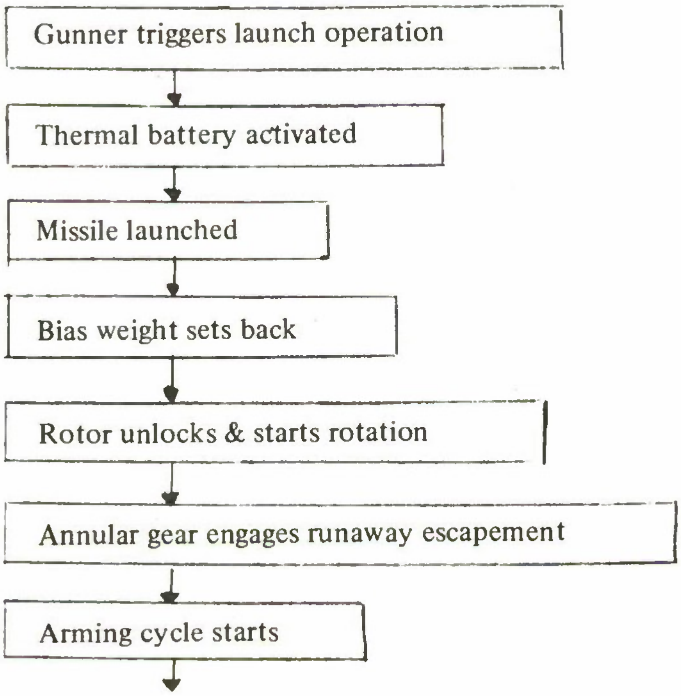
After launch, the missile is subjected to a uniform acceleration of X g's. During the application of this uniform acceleration force the arming mechanism controls the arming time. The arming time controls the arming distance which must fall between d and D feet.

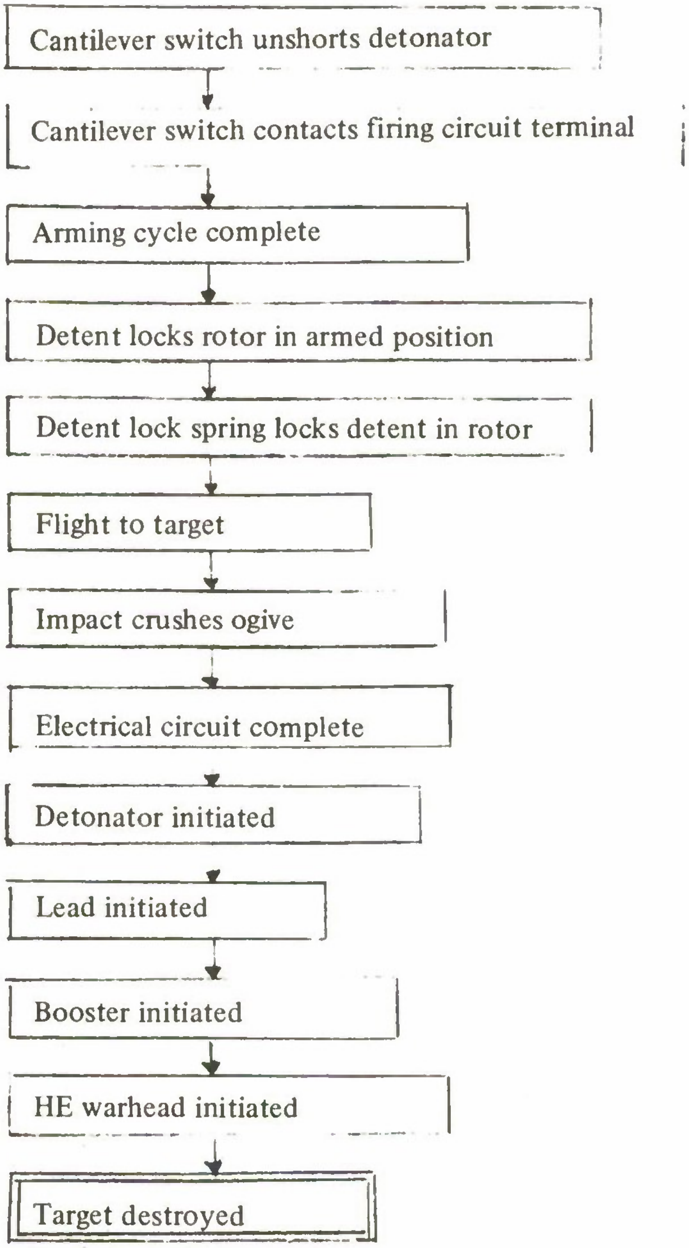
If at any time during the arming cycle the acceleration falls below N g's the S&A mechanism will recycle to the safe position.

Just before the rotor reaches the fully armed position the electrical cantilever switch unshorts the detonator and then makes contact with another terminal in the firing circuit. When the rotor reaches the fully armed position, the detent locks the rotor in position. When this happens the rotor cannot return to the safe position.

On impact the outer ogive contacts the inner ogive of the crush switch completing the electrical circuit. The electrical detonator is initiated, the detonator initiates the lead, the lead initiates the warhead booster and the booster initiates the HE warhead.

Block diagram of successful operation


Gunner triggers launch operation
Thermal battery activated
Missile launched
Bias weight sets back
Rotor unlocks & starts rotation
Annular gear engages runaway escapement
Arming cycle starts


Cantilever switch unshorts detonator
Cantilever switch contacts firing circuit terminal
Arming cycle complete
Detent locks rotor in armed position
Detent lock spring locks detent in rotor
Flight to target
Impact crushes ogive
Electrical circuit complete
Detonator initiated
Lead initiated
Booster initiated
HE warhead initiated
Target destroyed

Safety Requirements

1. The XM813 S&A device must withstand various combinations of storage, transportation, rough handling, and flight environments and remain safe and operable.

2. The S&A must not arm when subjected to a sustained (5 second) force caused by N g's or less.

3. The S&A must remain unarmed during the first d feet of flight.

4. The detonator must be shielded from stray RF energy.

5. The detonator must be shorted in the unarmed position.

6. The unit must be hand safe. If the detonator is initiated while the unit is unarmed, the housing must completely contain the detonation and the lead must not be initiated.

XM813 Safety Fault Tree Analysis

Two safety fault trees are shown for the XM813 S&A device.

a. Figure 12 shows the fault tree for a missile warhead which prematurely detonates in the gun tube.

b. Figure 14 shows the fault tree for a missile warhead which functions high order after it leaves the gun tube but less than the safe arming distance of d feet.

The Boolean Algebra solution for premature in gun tube (Fig 12) follows:

XM813 Fuze Prearmed

Start at Gate (7)

$$(7) = I . K$$

$$(6) = I . J$$

$$F = (5) = (6) + (7)$$

$$= I . J + I . K$$

$$E = (4) = G + H$$

$$C = (3) = D + E + F$$

$$= D + (4) + (5)$$

$$= D + G + H + IJ + IK$$

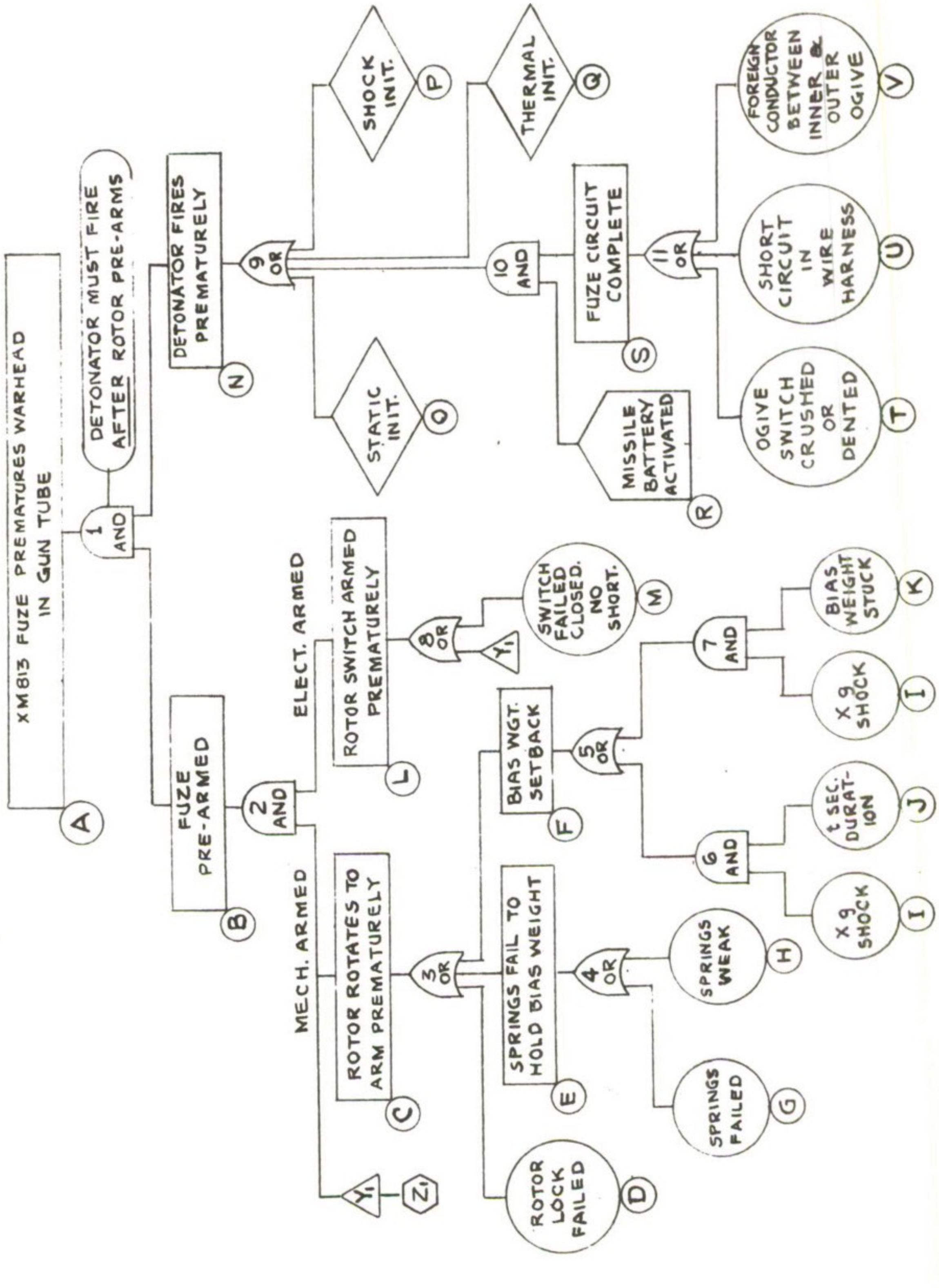

XM813 FUZE PREMATURES WARHEAD IN GUN TUBE
A
1 AND
DETONATOR MUST FIRE AFTER ROTOR PRE-ARMS
FUZE PRE-ARMED
B
DETONATOR FIRES PREMATURELY
N
2 AND
MECH. ARMED
ELECT. ARMED
ROTOR ROTATES TO ARM PREMATURELY
C
ROTOR SWITCH ARMED PREMATURELY
L
3 OR
Y1
Z1
8 OR
Y1
SWITCH FAILED CLOSED. NO SHORT.
M
ROTOR LOCK FAILED
D
SPRINGS FAIL TO HOLD BIAS WEIGHT
E
BIAS WGT. SETBACK
F
4 OR
SPRINGS FAILED
G
SPRINGS WEAK
H
5 OR
6 AND
X 9 SHOCK
I
t SEC. DURATION
J
7 AND
X 9 SHOCK
I
BIAS WEIGHT STUCK
K
9 OR
STATIC INIT.
O
SHOCK INIT.
P
THERMAL INIT.
Q
10 AND
MISSILE BATTERY ACTIVATED
R
FUZE CIRCUIT COMPLETE
S
11 OR
OGIVE SWITCH CRUSHED OR DENTED
T
SHORT CIRCUIT IN WIRE HARNESS
U
FOREIGN CONDUCTOR BETWEEN INNER & OUTER OGIVE
V

Fig 12 Safety fault tree

$\triangle Y_1 = C = (3)$ (Mechanically Armed)

$L = (8)$ (Electrically Armed)

$= Y_1 + M$

$B = (2) = C \,.\, L$

$= Y_1 \, (Y_1 + M)$

$= Y_1 \,.\, Y_1 + Y_1 \,.\, M$ But $Y_1 \,.\, Y_1 = Y_1$ Code IX

And $Y_1 = Y_1 \,.\, 1$ Code VI

$= Y_1 \,.\, 1 + Y_1 \,.\, M$

$= Y_1 \, (1 + M)$ But $(1 + M) = 1$ Code V

$= Y_1 \, (1) = Y_1$

$B = (2) = Y_1 = D + G + H + IJ + IK$

This means that any of the combined events listed under Y_1 would be enough to give an armed fuze prematurely (mechanically and electrically) and that event M only (switch fails closed) would not be a contributing cause. Because of the construction, a rotor which aligns the detonator with the lead would electrically arm the device.

Detonator Fires Prematurely

$(11) = S = T + U + V$

$(10) = R \,.\, S$

$= R \, (T + U + V)$

$= RT + RU + RV$

$N = (9) = O + P + Q + (10)$

$= O + P + Q + RT + RU + RV$

Fuze Prematures Warhead in Gun Tube

$$\begin{aligned} A &= (1) = B \cdot N \\ &= (2)\,(9) \\ &= (D + G + H + IJ + IK)(O + P + Q + RT + RU + RV) \\ &= DO + DP + DQ + DRT + DRU + DRV \\ &+ GO + GP + GQ + GRT + GRU + GRV \\ &+ HO + HP + HQ + HRT + HRU + HRV \\ &+ IJO + IJP + IJQ + IJRT + IJRU + IJRV \\ &+ IKO + IKP + IKQ + IKRT + IKRU + IKRV \end{aligned}$$

Safety Apportionment - XM813 Fuze Armed and Detonator Fires Prematurely in Gun Tube (Fig 12)

After having constructed a fault tree and written a Boolean Algebra expression for a premature in the gun tube, the next step is to quantify the expression. Since very little prior knowledge is available for the subject fuze, safety apportionment will be done as described on page 21.

Engineering Judgment

				Allowed Failures per Million
D	–	Rotor lock failed	.000006	(6/M)
G	–	Springs failed	.000004	(4/M)
H	–	Springs weak	.000005	(5/M)
I	–	X g shock	.1	(100,000/M)
J	–	t seconds duration	.001	(1,000/M)
K	–	Bias weight stuck	.00005	50/M)
O	–	Static initiation	.0000001	(.1/M)
P	–	Shock initiation	.00002	(20/M)
Q	–	Thermal initiation	.0000003	(.3/M)
R	–	Missile battery activated	1.0	(M/M)
T	–	Ogive switch crushed or dented	.001	(1,000/M)
U	–	Short circuit in wiring harness	.0003	(300/M)
V	=	Foreign conductor between inner and outer ogive	.00007	(70/M)

A = B . N

A = (D+ G + H + IJ + IK) (O+ P + Q + RT + RU + RV)

= (.000006 + .000004 + .000005 + .1x.001 + .1x.00005) (.0000001 + .00002 + .0000003 + 1x.001 + 1x.0003 + 1x.00007)

= (.000006 + .000004 + .000005 + .0001 + .000005) (.0000001 + .00002 + .0000003 + .001 + .003 + .00007)

= .000120 X .0013904 B = 120/M and N = 1390/M

= 1/8333 X 1/719

= .00000016685 = 1/5,993,260 (Probability of a premature functioning in the gun tube based on engineering judgment).

All Failure Modes Equally Likely

Assume safety requirement = 1 premature in 3,000,000 shots

A = 1/3,000,000

A = B . N

A = (D+ G + H + IJ + IK) (O+ P + Q + RT + RU + RV)
here R = 1.0 (normally expected)

Let X = each failure mode

A = $(X + X + X + X^2 + X^2)$ $(X + X + X + X + X + X)$

= $(3X + 2X^2)(6X) = 12X^3 + 18X^2$ = 1/3,000,000 = .0000003333

By trial and error X = .000136 = 1/7353

Check:

D =	= .000136	(136/M)
G =	= .000136	(136/M)
H =	= .000136	(136/M)
IJ = .000136 x .000136 = .000000018496		(.018/M)
IK = .000136 x .000136 = .000000018496		(.018/M)
.000408036992 = B = 1/2450		(408/M)
O,P,Q,T,U,V = 6 x .000136 = .000816	= N = 1/1225	(816/M)

A = B . N

A = .000408 x .000816 = .000000332928 vs .0000003333

Both Branches and Modes within Branches, Equally Likely

Assume safety requirement = 1 premature in 3,000,000 shots

$A = B \,.\, N = 1/1732 \times 1/1732 = 1/2{,}999{,}824$

$A = (D + G + H + IJ + IK)\,(O + P + Q + RT + RU + RV)$
here $R = 1.0$ (normally expected)

$B = (D + G + H + IJ + IK) = 1/1732 = .0005773$ (577/M)

Let X = each failure mode

$B = (X + X + X + X^2 + X^2) = .0005773$

$= 3X + 2X^2 = .0005773$

By trial and error $X = .0001924$

$N = (O + P + Q + RT + RU + RV) = 1/1732 = .0005773$

Let Y = each failure mode

$N = (Y + Y + Y + Y + Y + Y) = .0005773$ (577/M)

$= 6Y = .0005773$
$Y = .0000962$ (96/M)

Check:

D =	.00019240	(192/M)
G =	.00019240	(192/M)
H =	.00019240	(192/M)
IJ = .0001924 x .0001924 =	.000000037	(.037/M)
IK= .0001924 x .0001924 =	.000000037	(.037/M)
	.000577272	

O,P,Q,T,U,V = 6 x .0000962 = .0005772

$A = B \,.\, N = .000577 \times .000577 = .000000332929$ vs $.0000003333$

Sensitivity Rating (Fig 13)

$A = B \,.\, N$

$A = (D + G + H + IJ + IK)\,(O + P + Q + RT + RU + RV)$

Set all probabilities at .1 except $R = 1.0$ (normally expected)

$A = (.1 + .1 + .1 + .01 + .01)\ (.1 + .1 + .1 + .1 + .1 + .1)$

$= (.32)(.6) = .192$

Set each event at .5 - one at a time		Probability of output fault
D or G or H = $(.5 + .1 + .1 + .01 + .01)\ (.6)$	=	.432
I = $(.1 + .1 + .1 + .05 + .05)\ (.6)$	=	.240
J or K = $(.1 + .1 + .1 + .05 + .01)\ (.6)$	=	.216
O,P,Q,T,U,V = $(.32)\ (.5 + .1 + .1 + .1 + .1 + .1)$	=	.320

Event	Sensitivity Ratio	Sensitivity Rating
D,G,H	.432 ÷ .192	2.25
O,P,Q,T,U,V	.320	1.67
I	.240	1.25
J,K	.216	1.12

These sensitivity ratings are plotted on graph paper as the probability of output fault versus the probability of input fault. The plot is shown on Figure 13.

The above sensitivity rating table and Figure 13 show that events D, G,and H have more influence on the output fault than the other contributing events I, J,and K in Branch B and all of the events in Branch N.

Apportionment of the safety goal can be made to the failure modes and basic events so that D, G,and H will not influence event A any more than the other events. This is done by assigning fewer allowable probabilities of occurrence to D, G,and H. This can be accomplished in the following manner:

Using the sensitivity ratings, write the Boolean Algebra equation in one term with the highest rating. Let D be the term.

$$\frac{O,P,Q,T,U,V}{D} = \frac{2.25}{1.67} = 1.35$$

$O = 1.35D,\ P = 1.35D,\ Q = 1.35D,$ etc.

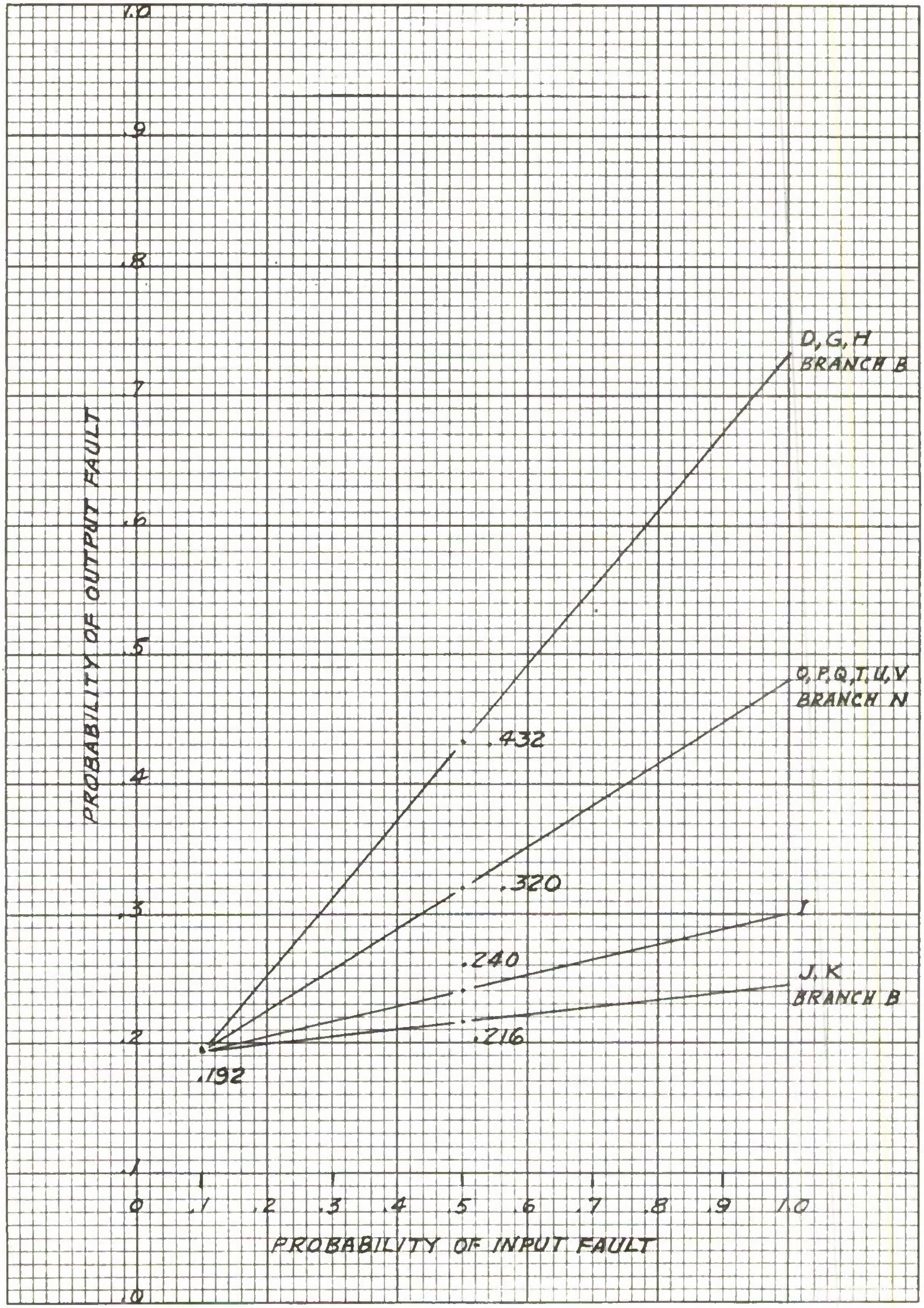


Fig 13 XM813 Sensitivity Ratio

$$\frac{I}{D} \quad \frac{2.25}{1.25} = 1.8 \quad ; \quad I = 1.8D$$

$$\frac{J,K}{D} = \frac{2.25}{1.12} = 2.0 \quad ; \quad J = 2.0D, K = 2.0D$$

$$A = B.N = (D+G+H+IJ+IK)\ (O+P+Q+RT+RU+RV) = \frac{1}{3{,}000{,}000}$$

$$A = (D+D+D+1.8D, \times 2.0D + 1.8D \times 2.0D)\ (1.35D + 1.35D + 1.35D + 1 \times 1.35D + 1 \times 1.35D + 1 \times 1.35D) = .0000003333$$

$$(3D + 7.2D^2)\ (6 \times 1.35D) = .0000003333$$

$$24.3D^2 + 58.32D^3 = .0000003333$$

By trial and error

$D = .000117$

Check:

Branch B

D = .000117	= .000117
G = .000117	= .000117
H = .000117	= .000117
IJ = 1.8 x .000117 x 2.0 x .000117	= .0000000493
IK = 1.8 x .000117 x 2.0 x .000117	= .0000000493
	.0003510986

Branch N

O	= 1.35 x .000117	= .000158
P	= 1.35 x .000117	= .000158
Q	= 1.35 x .000117	= .000158
RT	= 1 x 1.35 x .000117	= .000158
RU	= 1 x 1.35 x .000117	= .000158
RV	= 1 x 1.35 x .000117	= .000158
		.000948

A = B.N = .000351 x .000948 = .0000003327

SUMMARY

Branch B	**.000351**	**351/M**
D	= .000117	117
G	= .000117	117
H	= .000117	117
I	= .000210	210
J	= .000234	234
K	= .000234	234
Branch N	**.000948**	**948/M**
O	= .000158	158
P	= .000158	158
Q	= .000158	158
T	= .000158	158
U	= .000158	158
V	= .000158	158
R	= 1.0	1,000,000/M

All Major Events Equally Likely – Some Failure Modes Adjusted

Assume safety requirement = 1 premature in 3,000,000 shots

$A = 1/3{,}000{,}000$

$A = B\,.\,N = (D + E + F)(O + P + Q + R\,.\,S) = .0000003333$

(refer to Fig 12)

here R = 1.0 (normally expected)

Let X = each major event

$A = (X + X + X)(X + X + X + X)$

$\quad = (3X)\,(4X) = 12X^2 \qquad = .0000003333$

$X = \left(\frac{.0000003333}{12}\right)^{1/2} \qquad = (.0000000278)^{1/2} \quad = \quad .0001666$

Branch B = 3X = 3 x .0001666 = .0004998 (500/M)

D = .0001666

E = G + H = .0001666 (167/M)

Assume H = 1.3 times more likely to happen than G

$E = G + 1.3G = 2.3G = .0001666$

$G = \frac{.0001666}{2.3} = .0000725$ (72/M)

$H = E - G = .0001666 - .0000725 = .0000941$ (94/M)

Assume I twice as likely to happen as K and I eight times as likely as J.

$F = 1J + 1K = .0001666$

$= 1 \times \frac{1}{8} + 1 \times \frac{1}{2} = .0001666$

$= \frac{1^2}{8} + \frac{41^2}{8} = \frac{51^2}{8} = .0001666$

$I = (.0002665)^{1/2} = .0163266$ (16,327/M)

$J = \frac{1}{8} = \frac{.0163266}{8} = .0020408$ (2,041/M)

$K = \frac{1}{2} = \frac{.0163266}{2} = .0081633$ (8,163/M)

Branch N $= 4X = 4 \times .0001666 = .000666 = 1/1500$

$N = (O + P + Q + R \,.\, S) = .000666$ (666/M)

$O = .0001666$ (167/M)

$P = .0001666$ (167/M)

$Q = .0001666$ (167/M)

$S = \frac{R \,.\, S}{R} = \frac{1 \times .001666}{1} = .0001666$ (167/M)

$S = T + U + V = .0001666$

Event	**Rel. likelihood**	**Likelihood index**	**Safety apportionment**	
U	1.000 ÷ 2.166	.461	.0000768	(77/M)
T	.666	.308	.0000513	(51/M)
V	.500	.231	.0000385	(39/M)
	2.166	1.000	.0001666	

Branches Unequal and Failure Modes Adjusted

Assume safety requirement = 1 premature in 3,000,000 shots.

$$A = B \;.\; N = \frac{1}{1225} \times \frac{1}{2450} = \frac{1}{3,001,250}$$

$$A = (D + G + H + IJ + IK)\;(O + P + Q + RT + RU + RV)$$

here R = 1.0 (normally expected)

$$\text{Branch B} = \frac{1}{1225} \qquad (816/M)$$

Events, descending order	Relative likelihood	Likelihood index i	Safety apportionment iB	
IK	1.00 ÷ 3.20	.3125	.000255	(255/M)
D	.80	.2500	.000204	(204/M)
H	.65	.2031	.0001666	(166/M)
G	.50	.1563	.000128	(128/M)
IJ	.25	.0781	.000064	(64/M)
	3.20	1.0000	.000817	

Assume I twice as likely to happen as K

$$IK = 2K \;.\; K = 2K^2 = .000255$$

$$K = \left(\frac{.000255}{2}\right)^{1/2} = (.0001275)^{1/2} = .0112916 \qquad (11,292/M)$$

$$I = 2K = 2 \times .0112916 = .0225832 \qquad (22,583/M)$$

$$J = \frac{IJ}{I} = \frac{.000064}{.0225832} = .002833965 \qquad (2,834/M)$$

$$\text{Branch N} = \frac{1}{2450} \qquad (408/M)$$

Events, descending order	Relative likelihood	Likelihood index i	Safety apportionment iN	
U	1.000 ÷ 2.474	.404	.0001649	(165/M)
T	.666	.269	.0001098	(110/M)
V	.500	.202	.0000824	(82/M)
P	.260	.105	.0000429	(43/M)
Q	.036	.015	.0000061	(6/M)
O	.012	.005	.0000020	(2/M)
	2.474	1.000	.0004081	

Table 4

Failure mode safety apportionment allowed failures/million

	Engineering judgment	All failure modes equally likely	Both branches and modes within branches equally likely	Sensitivity rating	All major events equally likely and failure modes adjusted	Branches unequal and failure modes adjusted
Overall fuze safety	1/5,993,000	1/3,000,000	1/3,000,000	1/3,000,000	1/3,000,000	1/3,000,000
Branch B	120/M	408/M	577/M	351/M	500/M	816/M
D = Rotor lock failed	6	136	192	117	167	204
G = Springs failed	4	136	192	117	72	128
H = Springs weak	5	136	192	117	94	166
I = X g shock	100,000	136	192	210	16,327	22.583
J = t sec. duration	1,000	136	192	234	2,041	2,834
K = Bias wgt. stuck	50	136	192	234	8,163	11,292
Branch N	1390/M	816/M	577/M	948/M	666/M	408/M
O = Static initiation	.1	136	96	158	167	2
P = Shock initiation	20	136	96	158	167	43
Q = Thermal initiation	.3	136	96	158	167	6
T = Ogive switch crushed	1,000	136	96	158	51	110
U = Short circuit - Harness	300	136	96	158	77	165
V = Foreign conductor	70	136	96	158	39	82
R = MSL battery activated	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000

Discussion of Safety Apportionments

In the following discussion, the probability values assigned to the failure modes by Engineering Judgment will not be used since these values have the least substantiation.

In the other five categories each failure mode value was determined on the basic assumption that the minimum safety requirement for the complete fuze was one (1) premature in three million (3,000,000) shots.

Observe the values for failure mode D "Rotor Lock failed"

a.	For all failure modes equally likely	D = 136/M
b.	For both branches and modes within branches equally likely	D = 192/M
c.	Sensitivity rating	D = 117/M
d.	For all major events equally likely and failure modes adjusted	D = 167/M
e.	For branches unequal and failure modes adjusted	D = 204/M

From this, it can be seen that the least allowed rotor lock failures are 117 per million (c) and the most allowed failures are 204 per million (e).

To be ultra-conservative, the Safety Engineer can select each of the least allowed failures from the five situations as a safety goal for the individual events. By doing this, the S&A Device safety can be recalculated as follows:

Use Least Allowed Failures

$$A = B \cdot N$$

$$= (D + G + H + IJ + IK)\ (O + P + Q + RT + RU + RV)$$

here R = 1.0 (normally expected)

B

D =		= .000117
G =		= .000072
H =		= .000094
IJ =	.000136 x .000136	= .000000018
IK =	.000136 x .000136	= .000000018
	B	= .000283036

N

O		= .000002
P		= .000043
Q		= .000006
T		= .000051
U		= .000077
V		= .000039
	N	= .000218

A = B . N

A = .000283 x .000218 = .000,000,06169

$$A = \frac{.06169}{1,000,000} \times \frac{30}{30} = \frac{2}{30,000,000} \quad \text{(approx)}$$

This calculation shows that by using the least allowed failures for each event this particular system safety is five (5) times greater than the required safety goal.

By using all of the maximum allowed failures from the five situations, the system safety can be recalculated to show the poorest performance.

Use Maximum Allowed Failures

D	=		= .000204
G	=		= .000192
H	=		= .000192
IJ	=	.022583 x .002,834	= .000064
IK	=	.022583 x .001,292	= .000255
		B	= .000907

O	=	.000167	= .000167
P	=	.000167	= .000167
Q	=	.000167	= .000167
RT	=	1 x .000158	= .000158
RU	=	1 x .000165	= .000165
RV	=	1 x .000158	= .000158
		N	= .000982

A = B . N

A = .000907 x .000982 = .000000890674 = .89/M

$$\frac{89}{1,000,000} \times \frac{3}{3} = \frac{2.67}{3,000,000}$$

This value is approximately three (3) times worse than the safety goal of 1 in 3,000,000.

It is obvious that the allowed failure mode safety apportionments will lie somewhere between the least allowed and the maximum allowed failures for a given safety goal.

The question which the safety engineer must answer is: "Can the apportioned values be held within the limits?" If they can, then the safety requirements should be met. If it is likely that the apportioned values cannot be met, then some action must be taken to bring the failure rates of the critical components into line. Actions which may be taken could be:

a. Redesign of the components

b. Change of material

c. Better inspection

d. Better packaging

e. Redundant circuits

The Boolean algebra solution for Figure 14 follows:

XM813 Fuze Prematures Warhead at Unsafe Distance

S&A Device Armed Prematurely

$$C = \langle Z_1 \rangle = D + G + H + IJ + IK \quad \text{(From Fig 12)}$$

$$D_1 = (4) = E_1 + F_1 + G_1 + H_1$$

$$B_1 = (2) = C + D_1$$

$$= C + E_1 + F_1 + G_1 \quad H_1$$

$$= D + G + H + IJ + IK + E_1 + F_1 + G_1 + H_1$$

Detonator Fires

$$V_1 = (7) = K_1 + W_1$$

$$(6) = R \cdot V_1$$

$$= R\,(K_1 + W_1)$$

$$= RK_1 + RW_1$$

$$Q_1 = (5) = O + T_1 + (6)$$

$$= O + T_1 + RK_1 + RW_1$$

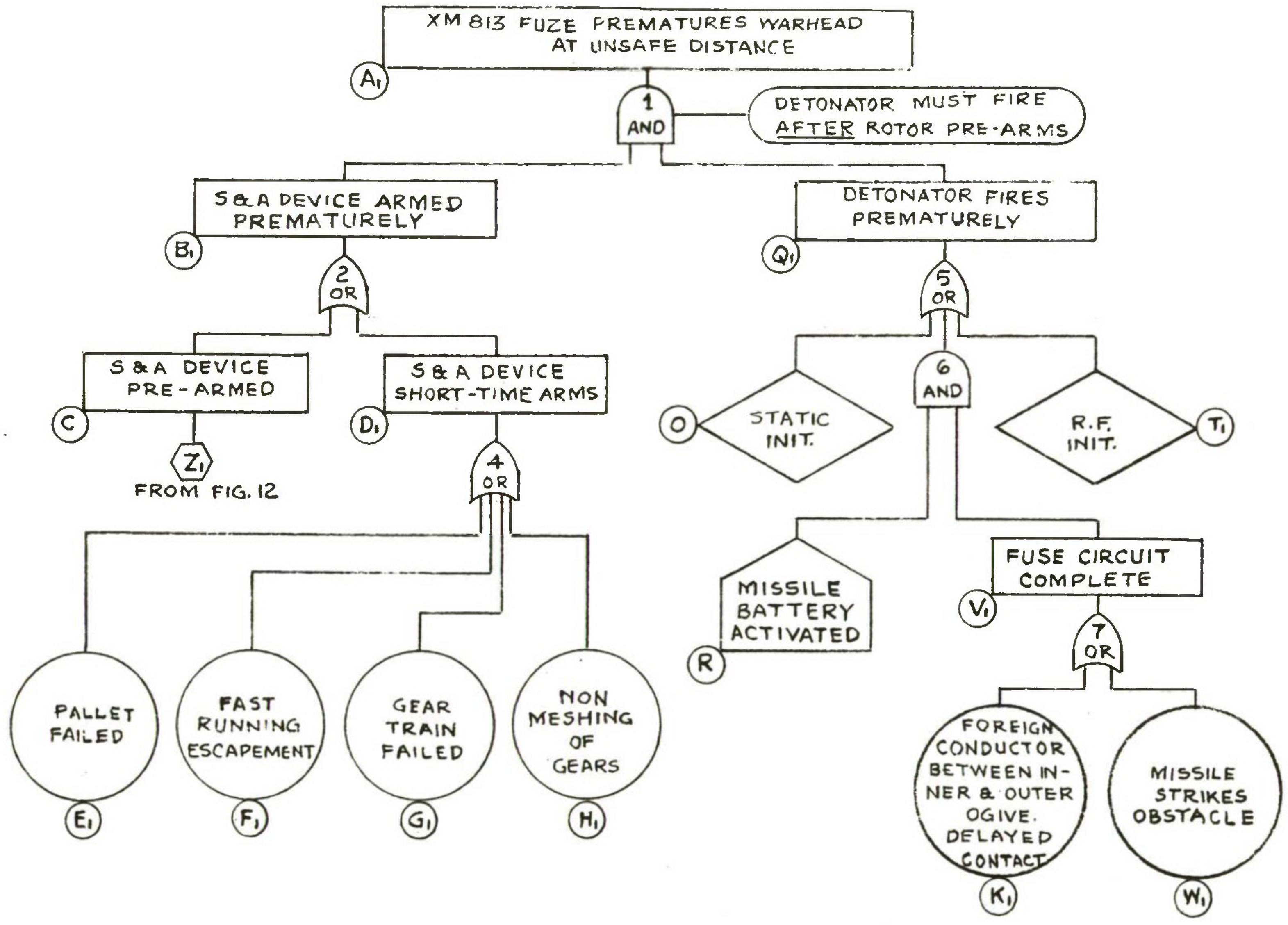


Fig 14 Safety fault tree

XM813 S&A Device Prematures Warhead at Unsafe Distance

$$\begin{aligned}
A_1 &= (1) = B_1 \;.\; Q_1 \\
&= (D + G + H + IJ + IK + E_1 + F_1 + G_1 + H_1) \\
&\quad (O + T_1 + RK_1 + RW_1) \\
&= O.(D + G + H + IJ + IK + E_1 + F_1 + G_1 + H_1) \\
+T_1 &\cdot (\qquad\qquad\qquad \text{''} \qquad\qquad\qquad) \\
+RK_1 &. (\qquad\qquad\qquad \text{''} \qquad\qquad\qquad) \\
+RW_1 &\cdot (\qquad\qquad\qquad \text{''} \qquad\qquad\qquad)
\end{aligned}$$

Any of the above combinations of events would cause the warhead to firc high order in lcss than the safe arming distance.

To illustrate one combination:

$E_1 \;.\; R \;.\; W_1 =$ Pallet failed *and* missilc battery activated *and* missile struck obstacle.

XM813 Reliability Fault Tree Analysis

Having considercd the many aspects of the construction and analyses of the *Safety* fault trees for the XM813 S&A Device, the construction of a *Reliability* fault tree will now bc undertaken. Figure 15 shows such a tree.

The XM813 S&A Device is a very simple mechanism of a series circuit type and there are no redundant circuits, so only OR gates appear on the fault tree. Also notice that there are no conditional gates. Sequence of occurrence is of no consequence.

The quantification of this fault tree would yield the *unreliability* of the device. The probability of success equals one minus the probability of failure (unreliability) and since reliability assessments of this type have been so well covered in many other documents, this step will not be discussed here.

Analysis of Figure 15

Start at Gate 2

$B = (2) = C + D + E + F$

$J = (5) = L + M + N$

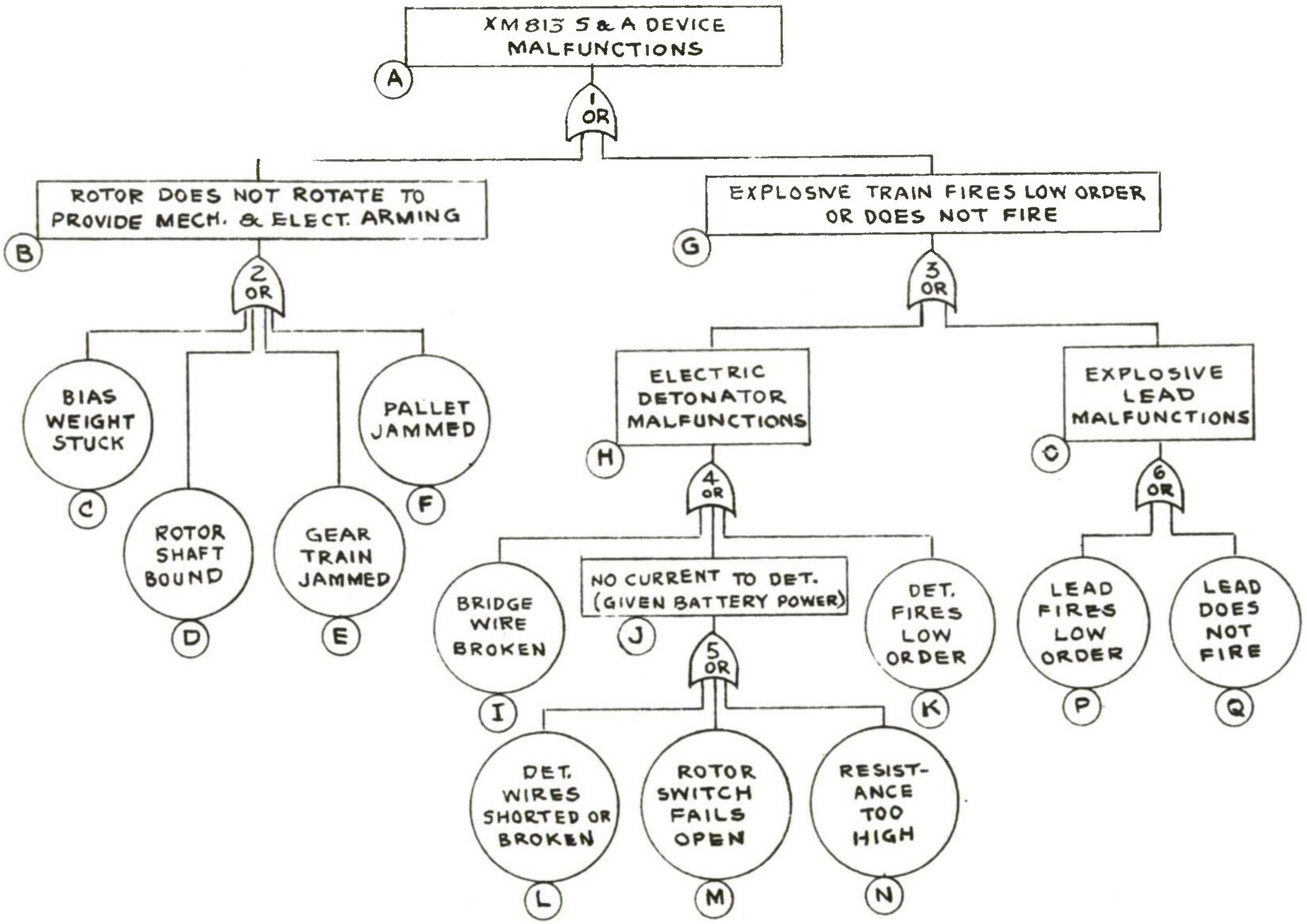

XM813 S & A DEVICE MALFUNCTIONS
A
1 OR
ROTOR DOES NOT ROTATE TO PROVIDE MECH. & ELECT. ARMING
B
2 OR
BIAS WEIGHT STUCK
C
ROTOR SHAFT BOUND
D
GEAR TRAIN JAMMED
E
PALLET JAMMED
F
EXPLOSIVE TRAIN FIRES LOW ORDER OR DOES NOT FIRE
G
3 OR
ELECTRIC DETONATOR MALFUNCTIONS
H
4 OR
BRIDGE WIRE BROKEN
I
NO CURRENT TO DET. (GIVEN BATTERY POWER)
J
5 OR
DET. WIRES SHORTED OR BROKEN
L
ROTOR SWITCH FAILS OPEN
M
RESIST-ANCE TOO HIGH
N
DET. FIRES LOW ORDER
K
EXPLOSIVE LEAD MALFUNCTIONS
O
6 OR
LEAD FIRES LOW ORDER
P
LEAD DOES NOT FIRE
Q

Fig 15 Reliability fault tree

$$
\begin{aligned}
H = (4) &= I + J + K \\
&= I + L + M + N + K \\
O = (6) &= P + Q \\
G = (3) &= H + O \\
&= I + K + L + M + N + P + Q \\
A = (1) &= B + G \\
&= C + D + E + F + I + K + L + M + N + P + Q
\end{aligned}
$$

Note: Any *one* of the above modes could cause the XM813 S&A Device not to function when required.

DISTRIBUTION LIST

	Copy Number
Commander	
US Army Materiel Command	
ATTN: AMCRD-W	1–3
AMCRD-D	4
AMCRD-ET	5
AMCSF-A	6
AMC-QC	7
5001 Eisenhower Avenue	
Alexandria, Virginia 22304	
Commander	
US Army Armament Command	
ATTN: AMSAR-EN	8
AMSAR-QA	9
AMSAR-SF	10
AMSAR-AS	11
AMSAR-SA	12
AMSAR-RD	13
AMSAR-Library	14–15
Rock Island, Illinois 61201	
Commander	
Picatinny Arsenal	
ATTN: SARPA-TS-T-S	16–20
SARPA-AD-P-A	21
SARPA-EO	22
SARPA-CO-T	23
SARPA-AD-D	24
SARPA-AD-E	25
SARPA-AD-F	26
SARPA-ND-D	27
SARPA-ND-E	28
SARPA-ND-N	29
SARPA-QA	30
SARPA-QA-A-A	31
SARPA-QA-A-P	32
SARPA-QA-A-S	33
SARPA-QA-A-F	34
SARPA-QA-A-M	35

SARPA-QA-A-R 36
SARPA-QA-T-C 37
SARPA-QA-N 38
SARPA-S 39
Dover, New Jersey 07801

Commander
US Army Test and Evaluation Command
ATTN: AMSTE 40
Technical Library 41–42
Aberdeen Proving Ground, Maryland 21005

Commander
US Army Electronics Command
ATTN: Library 43–44
Fort Monmouth, New Jersey 07703

Commander
US Army Aviation Systems Command
ATTN: AMSAV 45–46
P.O. Box 209, Main Office
St. Louis, Missouri 63166

Commander
US Army Mobility Equipment Command
ATTN: AMSME-ME 47–48
4300 Goodfellow Boulevard
St. Louis, Missouri 63120

Commander
US Army Tank Automotive Command
ATTN: AMSTA-RHFL 49–50
Warren, Michigan 48090

Commander
US Army Missile Command
ATTN: Redstone Scientific Information Center
Chief, Document Section 51–54
AMCPM-TOC (TOW) 55
AMCPM-MWC (DRAGON) 56
Redstone Arsenal, Alabama 35809

Commander
Natick Laboratories
ATTN: Technical Library 57
Kansas Street, Natick, Massachusetts 01760

Commander
US Army Materiel Command
ATTN: AMCPM-RK 58
Redstone Arsenal, Alabama 35809

Commander
US Army Materiel Command
ATTN: AMCPM-SA 59
Dover, New Jersey 07801

Director
US Army Aberdeen Research and Development Center
ATTN: Technical Library 60
Aberdeen Proving Ground, Maryland 21005

Commander
Edgewood Arsenal
ATTN: Technical Library 61–62
Edgewood, Maryland 21010

Commander
Frankford Arsenal
ATTN: Technical Library 63–64
SARFA-2000-QRI 65
Bridge-Tacony Streets
Philadelphia, Pennsylvania 19137

Commander
Watervliet Arsenal
ATTN: SWEWV-RDD 66
Watervliet, New York 12189

Commander
US Army Mobility Equipment R&D Center
ATTN: Technical Document Center 67–68
Fort Belvoir, Virginia 22060

Commander
Harry Diamond Laboratories
ATTN: Technical Library 69–70
Connecticut Avenue and Van Ness St., N.W.
Washington, DC 20438

Defense Documentation Center
Cameron Station
Alexandria, Virginia 22314 71–82

Commander
Naval Ordnance System Command
Department of the Navy
Washington, DC 20360 83

Commandant of the Marine Corps
Headquarters, US Marine Corps
ATTN: Code CSX-3 84
Washington, DC 20360

Commander
Naval Ordnance Laboratory
ATTN: Library 85
Code 433 – Room No. 2-135 86
White Oak, Maryland 20910

Commander
Naval Ordnance Laboratory
ATTN: Library 87
Corona, California 91720

Commander
Naval Ammunition Depot
ATTN: NAPEC 88
Crane, Indiana 27522

Commander
Naval Weapons Laboratory
ATTN: Library 89
Dahlgren, Virginia 22448

Commander
Naval Weapons Center
ATTN: Library 90
China Lake, Inyoken, California 93555

Commander
Naval Ordnance Station
ATTN: FS 71 A1 91
Indian Head, Maryland 20640

Commander
Naval Safety Center
Naval Air Station
ATTN: Code 1211 92
Norfolk, Virginia 23511

Commander
Naval Ship Research & Development Center
ATTN: Library 93
Annapolis, Maryland 21402

Headquarters
US Air Force
ATTN: AFSSSMB 94
Washington, DC 20330

Headquarters
Air Force Logistics Command
ATTN: MCNW 95
Wright-Patterson Air Force Base
Ohio 45433

Air Force Armament Laboratory
ATTN: DLOS 96
AFATL/DLDG 97
AFATL/ATZY 98
ADTC/ADAMP 99
Eglin Air Force Base
Florida 32542

Headquarters
Ogden Air Materiel Area
ATTN: MMEC 100
Hill Air Force Base, Utah 84401

Commander
Norton Air Force Base
ATTN: AFIAS-S 101
San Bernardino, California 92409

NASA Scientific and Technical Information Facility
Information Retrieval Branch
P.O. Box 33
College Park, Maryland 20740 102

National Aeronautics and Space Administration
ATTN: NASA Director of Safety 103
Washington, DC 20546

National Highway Traffic Safety Administration
400 7th Street, S.W.
Washington, DC 20590 104